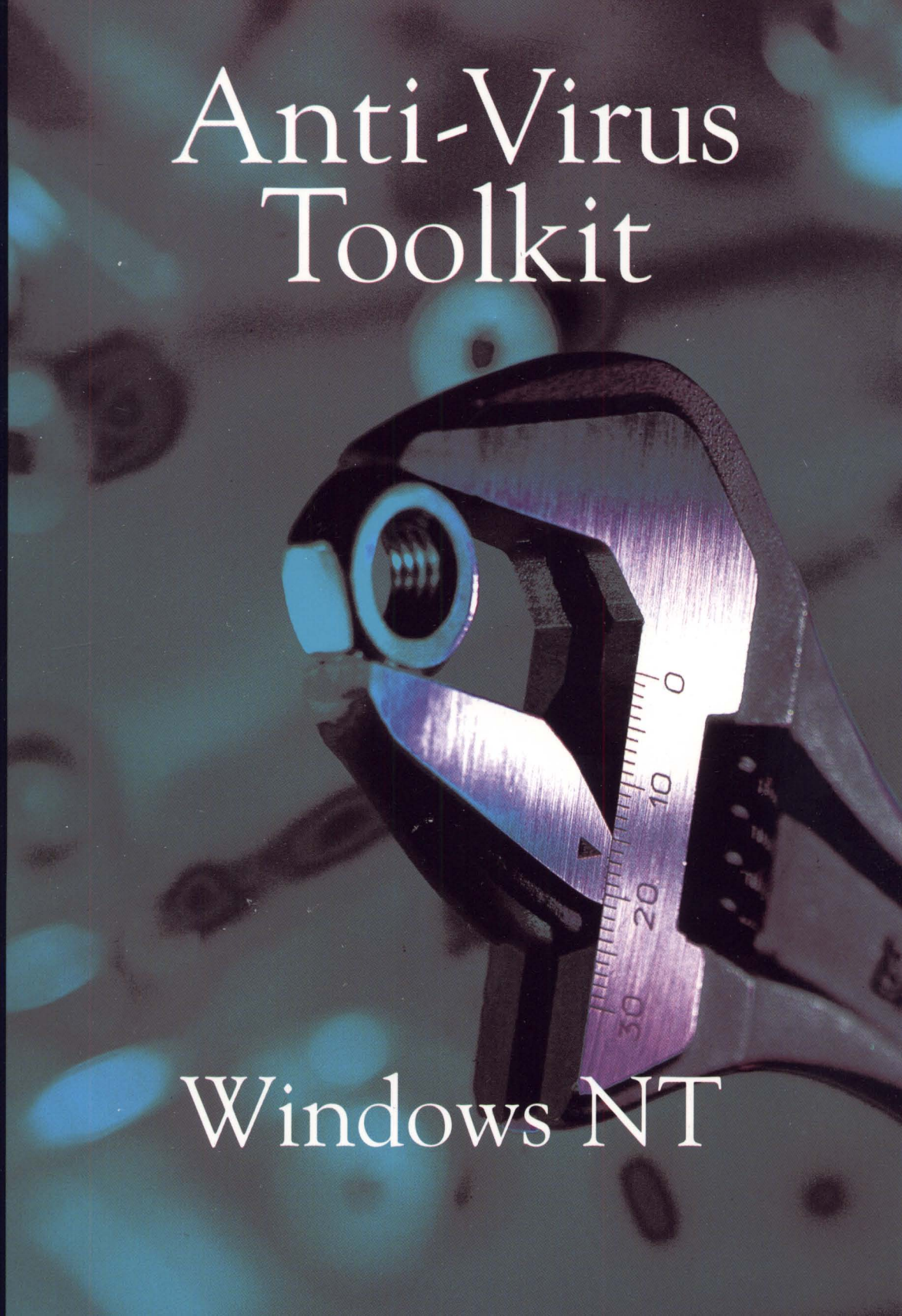
DR SOLOMON'S

Anti-Virus Toolkit



Windows NT

Dr Solomon's
Anti-Virus Toolkit

for Windows NT Workstation

S&S International PLC

Alton House, Gatehouse Way, Aylesbury, Buckinghamshire, HP19 3XU, UK

Tel: +44 (0)1296 318700 Fax: +44 (0)1296 318777

e-mail: support@uk.drsolomon.com

S&S Software International, Inc

1 New England Executive Park, Burlington, MA 01803, USA

Tel: +1 (1)617 273 7400 Fax: +1 (1)617 273 7474

e-mail: support@us.drsolomon.com

S&S Software International (Deutschland) GMBH

Luisenweg 40, 20537 Hamburg, Deutschland

Telefon: 040/251954-0 Fax: 040/251954-50

CompuServe: GO DRSOLOMON

SS1114A-20-05

Copyright

Dr Solomon's Anti-Virus Toolkit for Windows NT is copyright © 1996 S&S International PLC. All rights reserved. Dr Solomon's Anti-Virus Toolkit for Windows NT is not copy-protected. This does not mean that you can make unlimited copies of it. Dr Solomon's Anti-Virus Toolkit for Windows NT is protected by the copyright laws which pertain to computer software. It is illegal to make copies of the program other than as may be licensed or for purposes of backup without written permission from S&S International PLC. No part of the manual or other documentation accompanying Dr Solomon's Anti-Virus Toolkit for Windows NT may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language, in any form or by any means, without the prior written permission of S&S International PLC.

Disclaimer

Neither S&S International PLC nor anyone else who has been involved in the creation, production or delivery of Dr Solomon's Anti-Virus Toolkit for Windows NT or this manual makes any warranties with respect to the contents of the software or this manual and each specifically disclaims any implied warranties to the extent allowed by legislation. S&S International PLC reserves the right to revise the software and the manual and to make changes from time to time in the contents without obligation to notify any person.

Trademarks

Dr Solomon's is a registered trademark of S&S International PLC. All other product names mentioned are acknowledged to be the marks of their producing companies.

Software release

This manual describes version 7.5 of Dr Solomon's Anti-Virus Toolkit for Windows NT.

Manual edition

Edition 2.0
March 1996

Quickstart

If you need to act quickly, read the next two pages, especially if you think you may have a virus.

If you have bought the Toolkit because you suspect you might have a virus, the most important things to remember are:

- Don't panic.
- Don't rush into anything.

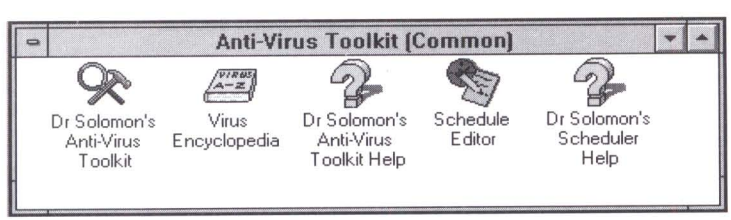
You could end up causing more damage than the virus.

Quick Installation

To install the Toolkit on your hard disk, follow these steps:

1. Start the PC as normal. Insert installation disk 1 in the A: drive.
2. From Program Manager, select Run from the File menu.
3. At the prompt, type `A:\SETUP` and press ↵. Follow the instructions displayed on the screen.
4. Follow the on-screen instructions carefully. At the end of installation, FindVirus will scan your local drives for viruses. If it finds a virus, it displays the virus name on the screen.

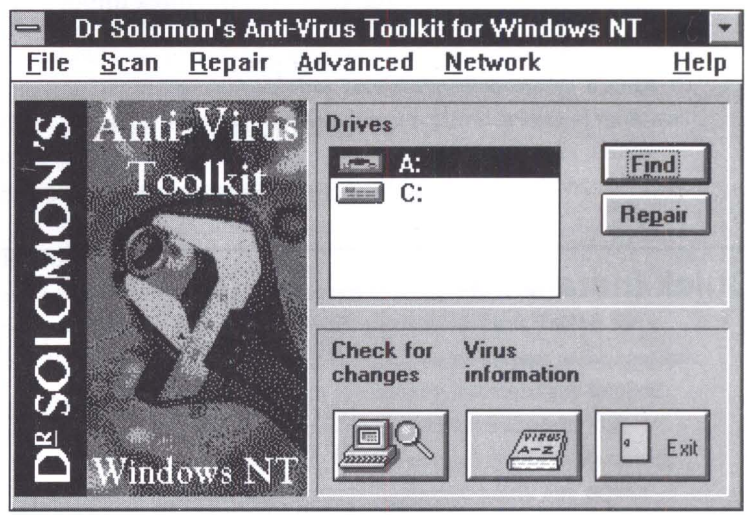
The Anti-Virus Toolkit group is created as follows:



Quick Repair

If you do have a virus, the simplest way to remove it is as follows:

1. Double-click on the Dr. Solomon's Anti-Virus Toolkit icon. The following screen appears:



2. In the Drives box, select the drive on which you suspect, or have found, a virus. Then select Repair.

The repair program checks the drive for viruses.

- Any infected files are repaired, if possible. If a file cannot be repaired, it is renamed. The first character of each file extension is changed to a V.
- If the boot sector of a diskette is infected, it is replaced with a clean boot sector.

The Repair program cannot repair infected boot sectors or partition sectors on hard disks. You need to reboot your system under DOS and run the DOS FINDVIRU.EXE executable with the 'repair' switch. DO NOT do this however if there is a possibility that an infected NTFS boot or partition sector may be found. If FindVirus tries to repair such a partition sector the data is likely to become corrupted. If a virus is reported in an NTFS boot or partition sector contact your local S&S International organisation for advice. When the repair is complete, run FindVirus again to check that the disk is free from viruses.

This page has been left blank

Contents

Contents i

Preface v
How to use this manual v
Conventions vii
What you need viii
Hardware requirements viii
Software requirements viii
Using the keyboard ix
Short-cut keys ix
Key functions ix
Related documentation x
The Virus Encyclopedia x
Other versions of the Anti-Virus Toolkit x
Registration and upgrades xii
If you need help xiii

1. Introduction 1
1.1 What is a virus? 1
1.2 Types of virus 2
File viruses 2
Macro viruses 3
Boot and partition sector viruses 3
Companion viruses 4
Overwriting viruses 4
Multipartite viruses 5
Droppers 5
1.3 Characteristics of viruses 5
Stealth 5
Polymorphism 5
Virus names 6
Variants 6
How viruses spread 6
1.4 Other potential problems 7
Bugs 7
Low-level software clashes 7
Trojans 8
Time bombs and logic bombs 9
Jokes 9
Human Error 9

1.5 What you can do 10
Backups 10
Software sources 11
Diskettes and other media 11
Employee co-operation 12
1.6 The Anti-Virus Toolkit 12
FindVirus 12
ViVerify 13
The Virus Encyclopedia 13

2. Installing the Toolkit 15
2.1 How to install the Toolkit 15
Installing the Scheduler 17
Completion of installation 18
Creating a rescue disk 19
2.2 README files 19
2.3 Upgrading the Toolkit 19

3. Finding your Way Around 21
3.1 Starting the Toolkit 21
3.2 The main screen 23
3.3 Options on the menus 23
File menu 24
Scan menu 24
Repair menu 25
Advanced menu 25

4. Checking for Viruses 27
4.1 Finding Viruses - FindVirus 27
When to use FindVirus 27
Running FindVirus from the main screen 28
Running FindVirus from the Scan menu 30
Advanced menu options 31
If FindVirus reports a virus 34
4.2 Checking for changes - ViVerify 35
When to use ViVerify 35
Running ViVerify 36
To create a file list 37
To compute the fingerprints 38
Checking the files 39
If a file has changed 39
Advanced menu options 40
4.3 The Virus Encyclopedia 43

5. Virus Repair and Removal 45
5.1 If you find a Virus 45
5.2 Single button repair 46
5.3 If you discover a new virus 47
5.4 Repair menu options 48
Repairing files 48
Replacing diskette boot sectors 50
5.5 Shredding files 52
5.6 Eradicating a virus 53
Planning the clean-up 53
Checking diskettes 55
Checking PCs 56

6. Using the Scheduler 57
6.1 The Schedule Editor 58
6.2 To set up a new event 60
Setting the event details 61
Scan settings 63
Frequency settings 65
6.3 Starting and stopping the Scheduler 66
6.4 Managing an event file 67
6.5 Activating an event file 67
6.6 The Toolkit Event Log 68
6.7 Setting up Scheduler defaults and options 68
General defaults 69
Scan Settings 70
List Boxes 71

7. Advanced Virus Detection 73
7.1 How FindVirus works 73
Executable files 74
Compressed and archived files 74
Repairing files 75
7.2 Running FindVirus from the user interface 76
7.3 Running FindVirus from the command line 76
Syntax 76
Scanning specific drives 80
Scanning files and subdirectories 81
Scanning network shares 82
Scanning compressed files 82
Scanning boot and partition sectors 83
Producing reports 83
Identifying viruses 84
Specifying actions 85
Network options 85

Defining drivers 87
Repairing files 87
Requesting extended errorlevels 89
7.4 Hints and Tips 90
Errorlevels 90
Hard disk device drivers 91
Scanning backup files 91
False alarms 91
7.5 Error messages 92

8. Advanced Virus Checking 95
8.1 How ViVerify works 95
Executable files 95
Encryption algorithms 96
Checking speed 96
Running ViVerify 97
8.2 Running ViVerify from the user interface 97
8.3 Running ViVerify from the command line 97
Syntax 97
Checking specific drives 99
Defining files to be checked 100
Specifying a fingerprint file 100
Excluding files 101
Checking boot and partition sectors 102
Specifying a keyword 102
Varying the checking speed and security 103
Specifying an algorithm 103
Defining actions 103
Producing reports 104
Extended errorlevels 104
Producing a list of suspect files 105
Errorlevels 105

9. Toolkit Configuration 107
9.1 The TOOLKIT.INI file 107
FindVirus 108
FileRepair 108
ViVerify 109
9.2 Configuration File Management 109

Glossary 111

Index 117

Preface

Dr. Solomon's Anti-Virus Toolkit for Windows NT contains everything you need to detect viruses, repair files and help prevent virus infection on your PC.

How to use this manual

This manual includes information for anyone using the Anti-Virus Toolkit for Windows NT, from the non-technical user to the PC expert. The sections you are interested in will depend on your level of knowledge and the information you need.

Chapters 1 and 2 are important for all readers. They provide background information on viruses and explain how to install the Toolkit.

Chapters 3 to 6 cover how to use the user interface and explain in detail the most straightforward ways to search for viruses and repair infected files.

Chapters 7 to 9 are aimed at more technical users. Read these if you want more in-depth information; for example, if you want to configure the tools for your particular needs.

If you do not have time to read the whole manual, particularly if you think you have a virus, read the Quickstart pages at the front of this manual.

Chapter 1 - Introduction explains what computer viruses are and the damage they can do. It explains the resources available in the Anti-Virus Toolkit to detect and remove viruses.

Chapter 2 - Installing the Toolkit gives step-by-step instructions for installing the Toolkit on your PC.

Chapter 3 - Finding Your Way Around shows you how to run the Toolkit programs, and explains the options that are available from each of the menus.

Chapter 4 - Checking for Viruses explains how to use the Toolkit to search for viruses on hard disks and diskettes.

Chapter 5 - Virus Repair and Removal explains the straightforward steps necessary to remove viruses and repair infections.

Chapter 6 - Using the Scheduler explains how you can set up virus checks and other programs to run at pre-set times.

Chapter 7 - Advanced Virus Detection provides detailed information on scanning for viruses using FindVirus.

Chapter 8 - Advanced Virus Checking provides detailed information on checking for changes in files using ViVerify.

Chapter 9 - Toolkit Configuration gives an explanation of the configuration files and how you can set them up and manage them.

A glossary is provided at the end of the manual, covering all the important terms used. There is also a comprehensive subject index.

Conventions

Throughout this manual, a number of conventions are used.

Information that you have to type is shown in the `Courier` typeface, for example:

```
WFINDV32 /LOCAL /DOALLFILES
```

Keys that you have to press are shown in the following form:

↓ Esc

↵ is used to indicate the Return or Enter key.

Throughout the text, symbols appear in the margin to draw your attention to particular points. These are as follows:

This indicates important information or tips to which you should pay particular attention.

This indicates a warning, and you should read it carefully.

What you need

Hardware requirements

The Anti-Virus Toolkit for Windows NT will run on PCs running Windows NT Workstation. It requires an Intel processor, and will not run on any other Windows NT hardware platforms.

It will run on a 486-DX-33 with 8 MB, although a Pentium with at least 16 MB is recommended for Windows NT.

Approximately 3 MB disk space is required.

Software requirements

The Anti-Virus Toolkit for Windows NT requires Windows NT Workstation v3.5 or above.

If you want to run the Toolkit on a network, or on more than one PC at a time, you should enquire about a site licence from S&S, or your international distributor if you are outside the UK.

The Anti-Virus Toolkit for Windows NT can detect all types of viruses. However, it cannot repair boot and partition sectors of hard disks. You need to reboot your system under DOS and run the DOS FINDVIRU.EXE executable with the `/REPAIR` switch at the command line. DO NOT do this however if there is a possibility that an infected NTFS boot or partition sector may be found. If FindVirus tries to repair such a partition sector the data is likely to become corrupted. If a virus is reported in an NTFS boot or partition sector contact S&S International for advice.

Using the keyboard

Since Windows NT was designed to be used with a mouse, it is strongly recommended that you use a mouse. However, all functions can be accessed from the keyboard if required.

Short-cut keys

Most Windows menu options can be selected by pressing short-cut key combinations, which are underlined.

Short-cut keys can always be used by pressing Alt + the short-cut key. For example, from the Toolkit user interface, pressing Alt + S displays the Scan drop-down menu.

Key functions

The keys that can be used within the Toolkit are as follows:

Key or combination	Function
↵	To accept a highlighted option button. The default button is normally OK.
Esc	To abandon a screen and return to the previous display.
Tab	To move to the next option in a dialog box.
Shift + Tab	To move to the previous option in a dialog box.
↓ ↑	Within a list of options, to move up and down the list.
Space	To select more than one item from a list.
F1	To display a screen of help text relevant to what you are doing.
Pg dn	To scroll down within the help text.
Pg up	To scroll up within the help text.

Related documentation

The Virus Encyclopedia

Included with your Toolkit is a copy of the Virus Encyclopedia book. As well as giving background information about viruses, it includes details of many of the viruses that the Toolkit can detect. The Encyclopedia categorizes each virus, describes its effects and explains how it can be removed. It also lists any alternative names by which the virus is known.

An on-line version of the Virus Encyclopedia is also included in the Toolkit. As new viruses are found, they are included in the latest Toolkit upgrade. The on-line version will always be more up-to-date than the printed copy.

Other versions of the Anti-Virus Toolkit

Windows and DOS

The Windows and DOS version of the Anti-Virus Toolkit provides virus detection, repair and protection facilities for all PCs running Windows 3.x or DOS 3.1 or above.

Novell NetWare

The NetWare version of the Anti-Virus Toolkit provides tools to protect NetWare servers and workstations from viruses. For complete protection, the package also includes the DOS/Windows version of the Toolkit.

OS/2

There are now specific viruses which can infect OS/2 systems. The Anti-Virus Toolkit for OS/2 provides full protection for OS/2 systems, detecting OS/2, DOS and Windows viruses. The package also includes the full DOS version of the Toolkit.

Windows 95

The Windows 95 version of the Anti-Virus Toolkit provides virus detection, repair and protection facilities for all PCs running Windows 95. The package also includes the full DOS version of the Toolkit.

SCO UNIX

The SCO UNIX version of the Anti-Virus Toolkit provides virus detection, repair and protection facilities for PCs running SCO UNIX. The package includes the DOS version of the Toolkit.

At the time of writing, versions of the Anti-Virus Toolkit are in preparation for Apple Macintosh, Windows 95 and SCO Unix. For more information, contact S&S or your authorized distributor.

Registration and upgrades

You will find a user registration card inside the Toolkit licence envelope. Complete the details on the card and return it to S&S or the representative in your country. If you do not register your purchase you will not receive upgrades to the Toolkit.

If you cannot find the registration card, call S&S or the representative in your country and quote the serial number on installation disk 1 of the Toolkit.

The virus researchers at S&S constantly receive specimens of new viruses for investigation, and the Toolkit is upgraded each month to take account of these. Typically, between 100 and 150 new viruses are reported every month. If your Toolkit is out-of-date, a message appears on the screen when you run the software, to remind you to upgrade.

For your own protection you should therefore subscribe to the regular software upgrade service. For many people, a quarterly upgrade offers sufficient protection, but if your system is at particular risk or if security is of major importance, monthly upgrades are also available.

You may have purchased a Toolkit with a pre-paid subscription for the first year of upgrades. In this case, once you register you will automatically be sent monthly or quarterly upgrades for 12 months from the date on the card.

If you don't send us the card, you will not receive the upgrades that you have already paid for.

If you didn't buy a pre-paid subscription, send the appropriate amount when you return your registration card. Full details are given on the card.

Send in your registration card.

If you need help

If you have a problem while installing or running the Toolkit, there are a number of ways in which you can obtain help.

Check the documentation carefully, including any README files on the disks as well as this manual and the help text. Make sure you have installed the software correctly. Your authorized distributor may also be able to advise you.

If you still cannot solve the problem, S&S support staff are available to help you. This service is free of charge.

You can contact S&S by any of the following methods:

UK Office

By telephone:	+44 (0)1296 318700
By fax:	+44 (0)1296 318734
By bulletin board:	+44 (0)1296 318810
By e-mail:	support@uk.drsolomon.com
By mail:	S&S International plc Alton House Gatehouse Way Aylesbury Buckinghamshire HP19 3XU United Kingdom

US Office

By telephone:	+1 617 273 7400
By fax:	+1 617 273 7474
By e-mail:	support@us.drsolomon.com
By bulletin board:	+1 (617) 229-8804

By mail:	S&S Software International Inc. 1 New England Executive Park Burlington, MA 01803 USA

German Office

By telephone:	+49 (0)40/251954-0
By fax:	+49 (0)40/251954-50
By e-mail:	support@de.drsolomon.com
By mail:	S&S International (Deutschland) GmbH Luisenweg 40 20537 Hamburg Deutschland

World Wide

By CompuServe:	GO DRSOLOMON
World Wide Web:	http://www.drsolomon.com/

When you contact S&S, it is helpful to have the following information available:

- Your name and company.
- Your serial number as printed on installation disk 1 of the Toolkit.
- The version of Windows NT you are using.
- The version number of the Toolkit you are using (this is printed on the label of the installation diskettes).
- A clean (that is, virus-free) write-protected DOS system boot diskette.

- In the case of an application error, any error messages reported.

If possible, you should be at the affected PC when you call us. We may need additional information, or we may ask you to carry out some diagnostic tests.

This page has been left blank

1. Introduction

Computer viruses are a growing problem. When S&S published the first version of the Anti-Virus Toolkit in 1989, the number of viruses at large in the world was in single figures. A year later, there were 50, and in the following year there were 200. By November 1995 there were over 7000. Between 100 and 150 new viruses are reported each month.

Many people panic when they hear the word *virus*. Remember though, computer viruses can be prevented, and if a virus infection is caught early it need not be particularly disruptive. The more preventive measures you can take the better, but you also need to be able to deal with a virus outbreak.

Dr. Solomon's Anti-Virus Toolkit for Windows NT will detect viruses and deal with virus infections. It detects and removes any known virus, that is, known in the current version of the driver file.

This manual also gives you some useful guidelines for establishing an anti-virus policy and for dealing with an outbreak, should one occur.

1.1 What is a virus?

Computer viruses are called viruses because they copy themselves. There are other types of software that can cause problems on your PC, and some of these are discussed in "Other potential problems" on page 7. However, no other type of software can replicate and it is this characteristic which makes a program a virus.

A virus is designed to copy itself without your knowledge. For example, it may attach itself to the FORMAT program and run every time you format a diskette.

If viruses do nothing but copy themselves, why are they such a problem?

Firstly, most viruses have deliberate or accidental side effects. Some of these seem harmless - they may simply display a message, make letters fall from the screen or play a tune. Others are specifically designed to be destructive, overwriting selected data or deleting files from the hard disk. In addition, many viruses do not operate as their authors intended them to because of bugs in the software; the side effects of these viruses are unpredictable. From the user's point of view, it does not matter whether the damage caused by a virus was a deliberate act by the virus author or an error in the program.

Secondly, most viruses stay in your PC's memory where they can cause problems by interfering with other software.

Thirdly, once you have a virus, it is very likely that you will unwittingly pass it on to a colleague or a customer, who may well lose confidence in you and your organization.

No virus is completely harmless; they all waste your time, processor time, memory and disk space. Dr. Solomon's Anti-Virus Toolkit for Windows NT can help insure that your PC remains free from such disruption and from virus infection.

1.2 Types of virus

At present, there are no specific Windows NT viruses. However, NT systems are vulnerable to attack from DOS and Windows viruses. The different types of virus, and the damage they can do, are outlined below.

File viruses

File viruses infect executable program files; these may include some data files containing executable macros. These usually, but not always, have COM or EXE file extensions. When you run an infected program the virus runs first, then passes control

to the original program. While it has control, the virus code copies itself to another file or to another disk, replicating itself.

On Windows NT systems, a file virus can run whenever a DOS application is run, either within a DOS emulation window, or by running a DOS or 16-bit Windows executable file. Once running, many file viruses go memory-resident (also known as TSR, or Terminate and Stay Resident programs). Once in memory, the virus infects every program that is subsequently run. It can also interfere, deliberately or accidentally, with the operation of other memory-resident programs. When the DOS window is closed, the virus terminates, but it may already have infected files and corrupted data. Note that under Windows NT, a virus may not have the same effect as it does under DOS. In particular, viruses will not be able to write to hard disk boot and partition sectors from within the DOS emulation environment.

Some viruses do not load into memory. Instead, when the infected program is run, they infect another program.

Macro viruses

There are now macro viruses in existence, for example the Winword.Concept virus that infects Word 6 document files. This virus can infect Word 6 on any operating system including Windows NT. Many applications now have similar macro languages which could potentially be used to create viruses in the future.

Boot and partition sector viruses

The partition sector is the first part of a hard disk to be read after the system has started up. It contains information about the disk such as the number of sectors in each partition and the location of all the partitions. The partition sector is also called the Master Boot Record (MBR).

The boot sector is the part of every hard disk and diskette which is read by the computer when it starts up. The boot sector of a system disk contains the code necessary to load the

system files; a data disk contains the code necessary to display the message that the PC cannot be booted from that disk.

Most PCs are set up to attempt to boot from the A: drive first. If the boot sector of a diskette is infected, the virus runs when you attempt to boot from the diskette, and infects the hard disk.

For example, if you leave a non-system diskette in the drive overnight and then switch on your PC the next day, the following message, or similar, is displayed:

```
Non-system disk or disk error
Replace and press any key when ready
```

If the diskette is infected with a boot sector virus, that virus has already run, and your PC may already be infected.

Any Intel-based PC is vulnerable to boot and partition viruses. They can infect any PC, regardless of the operating system, since the virus runs before the system starts up.

On a Windows NT system, many boot sector viruses corrupt the partition sector and prevent the system from subsequently booting normally. Others may crash or hang the system or corrupt the file system. A few will allow Windows NT to boot normally but none known to S&S at the time of going to press are able to survive the boot process and replicate.

Companion viruses

If you have a COM file and an EXE file of the same name, DOS always runs the COM file in preference to the EXE file if no file extension is given. Companion viruses make use of this fact by creating COM files with the same name as the legitimate EXE files, thus ensuring they are executed. They then pass control to the original EXE file which runs normally. Companion viruses will run in the Windows NT DOS emulation environment.

Overwriting viruses

An overwriting virus simply overwrites each file it infects with itself, so the program no longer functions. As this is very easy

to spot, these viruses do not spread well, and are not a real threat. Overwriting viruses will run in the Windows NT DOS emulation environment.

Multipartite viruses

Some viruses use a combination of techniques to spread, and may infect executable files, boot sectors and partition sectors. These will generally not be able to spread under Windows NT.

Droppers

A dropper is a program, not a virus itself, that installs a virus on the PC while performing another function. Droppers that attempt to spread boot sector viruses will not work under Windows NT.

1.3 Characteristics of viruses

Stealth

Although some virus infections are readily apparent to the user, the most successful viruses try to remain as inconspicuous as possible so that they can spread without being noticed. A virus which uses *stealth* is one that tries to conceal its presence on the disk so that everything appears to be running normally. Many boot sector viruses use a certain amount of stealth; after running they pass control to the original boot sector so that the PC starts up normally. A detailed discussion of stealth, and ways to counteract it, is in the Virus Encyclopedia.

Polymorphism

Many virus detection programs work by looking for a known pattern of bytes in the code of the virus. A *polymorphic* virus is one that tries to avoid detection in this way by insuring that its code does not have a fixed pattern of characters. Usually the virus achieves this by encrypting itself differently each time it runs.

The Toolkit can deal effectively with polymorphic viruses using the Generic Decryption Engine. This can decrypt the virus without knowing the encryption method, allowing virus-scanning software to identify the virus and repair the infected files. It achieves this rapidly and without any time-wasting false alarms. The Generic Decryption Engine is built into the Toolkit's scanner, FindVirus.

More information on polymorphic viruses is given in the Virus Encyclopedia.

Virus names

Many viruses appear to have several different names. This happens because most viruses are named by the anti-virus researchers who identify them, rather than by their authors, who prefer to remain anonymous. Different researchers often give viruses different names, based on text within the virus code or where they were first discovered.

S&S uses names which are approved by the Computer Anti-Virus Researchers Organization (CARO). In addition, the Virus Encyclopedia lists any aliases by which the virus is commonly known.

Variants

Many viruses are found in a number of related variations, often because their authors have simply altered the code of existing viruses. The Virus Encyclopedia includes details of many known variants which the Toolkit is able to find and deal with.

How viruses spread

The most common way in which a virus is spread is via an infected diskette. Boot sector viruses are the most common type of virus, and they can only be transmitted by a diskette. People who use diskettes on a number of different PCs increase their chances of picking up an infected diskette and spreading the virus.

Some people mistakenly assume that shareware, free disks and games are the only sources of viruses. Although viruses are sometimes transmitted through these types of software, because they tend to be copied more, they have also been found in shrink-wrapped software distributed by major companies, and on diskettes accompanying hardware. For this reason, you should always scan all diskettes for viruses before they are used.

File viruses can also be spread by downloading infected programs from bulletin boards. You should take care to check any software transferred over a network or communications link before using it.

A workstation on a network can be infected in the same way as a standalone PC, and a virus can spread very quickly across a network. As the effect of a virus infection can be particularly serious if a file server becomes infected, you should take extra care to protect networks from infection.

1.4 Other potential problems

When something goes wrong with a PC, it is easy to think it must be a virus. Unfortunately, there are many other problems which can disrupt work and destroy data. Some of these are described below.

Bugs

A bug is an unintentional fault in a program. Virtually all complex software contains bugs. Minor bugs merely cause inconvenience, while major bugs can cause catastrophic data loss. There is no way of detecting bugs, and the only defense is to insure you back up your important data regularly.

Low-level software clashes

Low-level programs are those which work on disks directly. They are so-called because they function below the level of the

operating system, which normally controls access to disks and enforces certain rules. Low-level programs include:

- Disk sector editors.
- Disk caching programs.
- Disk compression software.
- Defragmenters.

These tools are usually fairly safe to use if you only run one at a time, but problems can occur if you run two or more low-level tools at the same time. If two or more tools try to access the disk, potentially dangerous clashes can result. As these tools become more common, this type of problem is more and more likely to occur.

To avoid problems with low-level tools:

- Always take a backup before using any disk utilities.
- Do not run more than one utility at the same time.
- Avoid using these tools at the same time as using memory-resident software.
- Always read the manuals and any README files supplied with the product. If the manufacturer has included any special warnings, there is usually a good reason for them!

Trojans

Trojans are programs that do something unexpected and usually damaging. They are less widespread than viruses because they do not replicate, but they can represent a threat when copied. Many people confuse the two - the AIDS Information Diskette, often cited by the media as an example of a virus, was actually a trojan. Also, viruses sometimes contain trojans.

You are unlikely to encounter a trojan if you always obtain your software from reputable sources, but the main defense against damage by such programs is to back up your system.

The Toolkit finds and identifies some known trojans and treats them in the same way as viruses.

Time bombs and logic bombs

These are particular types of trojan. A time bomb is set off on a particular date, while a logic bomb is triggered by a specific set of conditions, such as the number of files on a disk or a certain sequence of characters being entered. Both types usually do something damaging.

Jokes

Some programs claim to be doing something destructive to your computer, but are actually harmless jokes. For example, a message may appear suggesting that your hard disk is about to be reformatted. Unfortunately, it is easy to over react to the joke and cause more damage by trying to eradicate something that is not, in fact, a virus.

The Toolkit finds and identifies a number of widespread joke programs.

Human Error

When something goes wrong with your PC, or you lose data, the most likely cause is not a virus or a software problem, but human error. Everybody makes mistakes such as pressing the wrong key sequence or typing DEL *.* in the wrong directory, and these can have drastic results.

Remember that the most valuable part of your computer is the data you have stored on it. Hardware and programs can be replaced but you can only replace your data if you have backed it up.

1.5 What you can do

The data recovery specialists at S&S in the UK see a lot of people who have lost their data. Fortunately, the data can nearly always be restored and we can usually identify the reason that it was lost in the first place.

Although viruses are a problem, the scale of the problem should be kept in perspective. The most common reason for losing data is human error. The second most common cause is hardware failure, followed by software problems and bugs. Viruses come a poor fourth.

However, implementing a straightforward anti virus policy will help protect your data from all kinds of loss, including viruses. In particular, you should consider the following three elements of protection:

- **Prevention** - to limit the spread of viruses.
- **Detection** - to insure that if a virus does get through the defenses, it is discovered as quickly as possible.
- **Recovery** - to insure that if any files are lost or damaged, they can be restored as quickly as possible.

Using the Anti-Virus Toolkit is obviously a significant part of the detection and recovery policy, but some other elements of a sensible anti virus policy are suggested below.

Backups

The most important precaution you can take against any kind of data loss is to make regular backups of your system. If you do not back up your data regularly, it is at risk.

Remember to check your backups frequently and make sure that you can restore your data from them.

Check that you have clean copies of all your executable files on diskette. All your backup diskettes and your boot diskettes should be write-protected.

Software sources

Make sure that all your software comes from a reputable source. Check that software is in its original packaging.

Never use pirated software. Even if you feel entitled to use another copy temporarily (for example, because you left your licensed copy at another site) remember that the copy may expose you to virus infection.

Software can enter your PC via the communications ports as well as via portable media. Take care when transferring software to and from laptops and across networks and when downloading files from bulletin boards.

Diskettes and other media

The risk of virus infection via diskette is particularly high, but you can take some simple steps to increase security.

- Keep diskettes write-protected wherever possible, to prevent viruses being copied onto them.
- Do not leave a diskette in the drive when you turn off the PC. This will prevent booting from an infected diskette.If you do accidentally boot from a non-bootable diskette, switch off and start again instead of proceeding with the boot from the C: drive.
- Change the CMOS setting of your PC so it boots from the C: drive first rather than the A: drive. (This is not always possible on SCSI drives).
- Use alternative methods of file transfer where possible.
- Remember that files on tape may have been infected when the back-up was made.

Employee co-operation

You need the willing co-operation of your employees in any anti-virus policy. If members of staff think that they are likely to be disciplined if they discover a virus, they are unlikely to report any problems.

Some companies have attempted to ban the playing of games. It is a much better policy to insure that games come from a reputable source and are checked before use. It can be useful to give one person or a small group the responsibility of checking and distributing games software.

1.6 The Anti-Virus Toolkit

The Anti-Virus Toolkit for Windows NT provides a set of tools for the detection and removal of viruses. There are two major types of anti virus software.

- A *scanner* is a program that searches for viruses. As new viruses are continually appearing, scanners need to be updated regularly.
- A *checksummer* detects changes in files. It calculates a unique numeric fingerprint, known as a checksum, for each file to be protected. The checksummer can then re-calculate this fingerprint to monitor any differences. Executable files do not usually change, so if there is a difference in the fingerprint, a virus may be present.

Dr. Solomon's Anti-Virus Toolkit for Windows NT includes both a scanner and a checksummer; these operate as described below.

FindVirus

FindVirus is a scanner that you can use regularly to scan your hard disks and any incoming diskettes. It will find and report any virus known to the current version of the driver file. It also includes an optional heuristic analyzer that looks inside files for

suspicious code that may indicate a previously unknown virus.

FindVirus will find viruses in files, boot sectors, partition sectors. It can also be used to repair virus infections. FindVirus can be used to scan incoming diskettes and files on a footbath PC - one that is always used for that purpose. FindVirus scans very quickly and can be used for scanning hard disks on a daily basis.

ViVerify

ViVerify is a checksummer that detects changes in executable files that may have been caused by a virus infection. Initially you can use ViVerify to calculate a fingerprint, or checksum, for each file. You can then run ViVerify regularly to re-calculate this fingerprint and check if there are any changes. Although a change to an executable file does not necessarily mean that the file is infected, executable code does not normally change. ViVerify reports any possible virus, even a previously undiscovered one.

The Virus Encyclopedia

The on-line Virus Encyclopedia includes details of the most common viruses which the Toolkit can detect, including any variants. The on-line Virus Encyclopedia is more comprehensive than the Encyclopedia manual.

This page has been left blank

2. Installing the Toolkit

This chapter explains how to install the Anti-Virus Toolkit for Windows NT on your workstation.

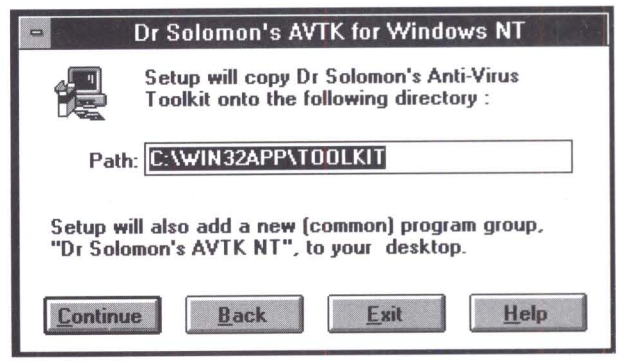
Before using the Toolkit, you should make a copy of the program disks as a backup. Note that the terms of your license agreement allow you to make one copy only.

2.1 How to install the Toolkit

To install the Toolkit, follow the steps below.

1. Start up your PC as normal and logon with a username which is in the administrator group.
2. If you are not upgrading from an earlier version of the toolkit jump to Step 6. If you are upgrading from an earlier version carry on with the next step.
3. Find the Dr Solomon's AVTK NT program group and delete the Dr Solomon's Scheduler item, if it is present.
4. Find the Startup group and delete the Dr Solomon's Scheduler item, if it is present.
5. Find the toolkit directory (usually \WIN32APP\TOOLKIT) and delete the file TK_SCHED.EXE.
6. Insert the WINDOWS NT installation diskette 1 into the A: drive.
7. From Program Manager, select Run from the File menu.
8. At the prompt, type `A:\SETUP` and press ↵. Follow the instructions on the screen.

9. You will be prompted to confirm the installation path:

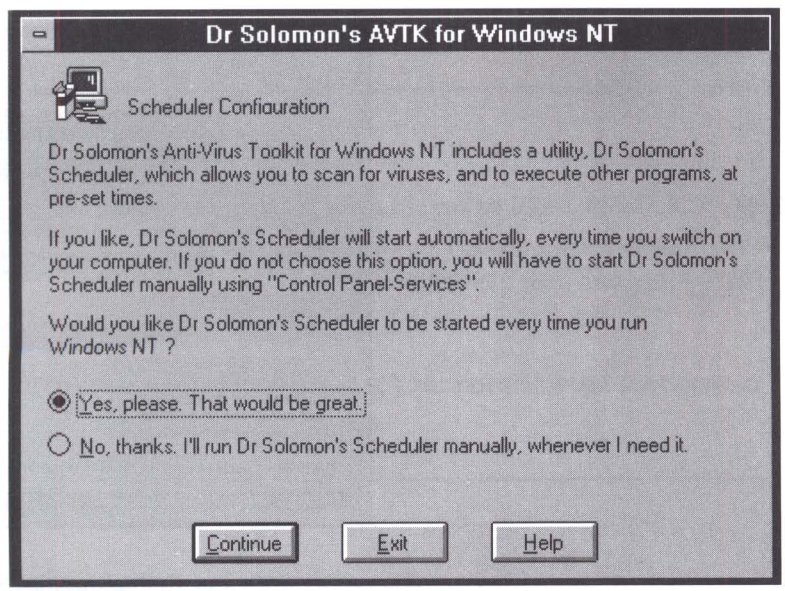

Dr Solomon's AVTK for Windows NT
Setup will copy Dr Solomon's Anti-Virus Toolkit onto the following directory :
Path: C:\WIN32APP\TOOLKIT
Setup will also add a new (common) program group, "Dr Solomon's AVTK NT", to your desktop.
Continue
Back
Exit
Help

   Enter an alternative path if you wish and press ↵. The installation process starts.

You are prompted to insert further disks during the installation process. You can cancel the installation at any time by pressing Esc. If you then want to re-install, you should delete any files in the Toolkit directory that were created in the original installation.

Installing the Scheduler

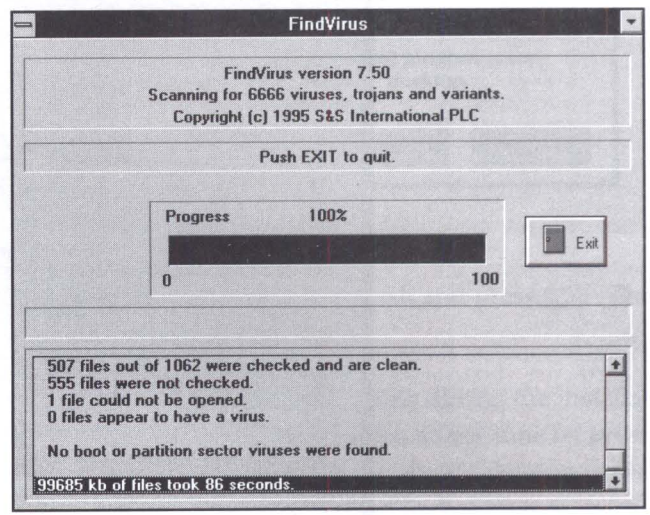
When the main Toolkit files have been installed, you will be asked whether you wish to run Dr. Solomon's Scheduler every time you use Windows NT.


Dr Solomon's AVTK for Windows NT
Scheduler Configuration
Dr Solomon's Anti-Virus Toolkit for Windows NT includes a utility, Dr Solomon's Scheduler, which allows you to scan for viruses, and to execute other programs, at pre-set times.
If you like, Dr Solomon's Scheduler will start automatically, every time you switch on your computer. If you do not choose this option, you will have to start Dr Solomon's Scheduler manually using "Control Panel-Services".
Would you like Dr Solomon's Scheduler to be started every time you run Windows NT ?
Yes, please. That would be great.
No, thanks. I'll run Dr Solomon's Scheduler manually, whenever I need it.
Continue
Exit
Help

If you want more information on starting the scheduler manually before making a choice, see "Starting and stopping the Scheduler" on page 66.

Completion of installation

When the installation process is complete, FindVirus runs automatically to scan your local hard disks for any viruses. If your PC is free from viruses, a screen similar to this is displayed:


FindVirus
FindVirus version 7.50
Scanning for 6666 viruses, trojans and variants.
Copyright (c) 1995 S&S International PLC
Push EXIT to quit.
Progress 100%
0
100
Exit
507 files out of 1062 were checked and are clean.
555 files were not checked.
1 file could not be opened.
0 files appear to have a virus.
No boot or partition sector viruses were found.
99685 kb of files took 86 seconds.

The report indicates that some files have not been checked. This is because, by default, FindVirus only checks executable files, as data files cannot be infected by viruses. For more information on FindVirus, see "Finding Viruses - FindVirus" on page 27.

The installation is now complete, and your PC has been scanned for viruses. Press any key to return to the Windows Program Manager.

If FindVirus reports a virus on your PC, do not panic! See Chapter 5, "Virus Repair and Removal", for information about what to do.

If you have problems installing the Toolkit, check that you have followed the procedure in this manual. If you cannot resolve

the problem, contact S&S Technical Support. See "If you need help" on page xiii.

Creating a rescue disk

After installing the toolkit you are STRONGLY RECOMMENDED to create a rescue disk. You can do this using the RDISK.EXE utility supplied with Windows.

2.2 README files

As part of the installation, a file called README.DOC is copied to the Toolkit directory. This file contains information that is not included in the manual or the help text, and you should read it carefully.

You can open this file using your normal word processor or editor.

2.3 Upgrading the Toolkit

The Toolkit is updated monthly to deal with new viruses. We recommend that you maintain a subscription to the upgrade service to insure complete protection from viruses. See "Registration and upgrades" on page xii.

Upgrades are available on a quarterly or monthly basis, and consist of a complete set of disks. To install the upgrade:

1. Insert the WINDOWS NT installation diskette 1 into the A: drive.
2. From Program Manager, select Run from the File menu.
3. At the prompt, type `A:\SETUP` and press ↵. Follow the instructions on the screen.

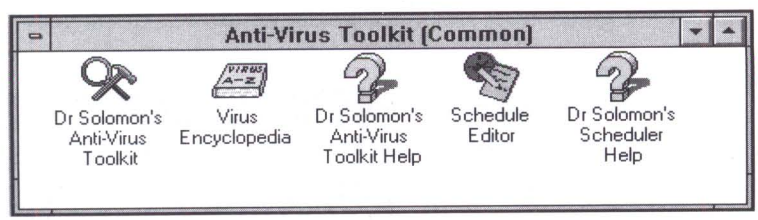
This page has been left blank

3. Finding your Way Around

This chapter explains how to start up and use the Toolkit. It covers the options available from the menus and how to move around the user interface.

3.1 Starting the Toolkit

When the Windows installation is complete, the Anti-Virus Toolkit program group appears:



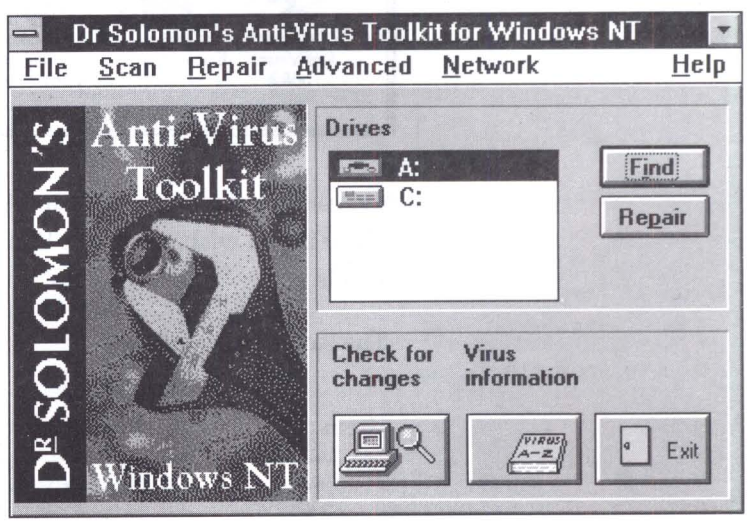
You can of course move the Toolkit icons to another program group if you wish. See your Windows documentation for full details.

The icons are as follows:

Item	Purpose
Dr Solomon's Anti-Virus Toolkit	Starts the Toolkit and displays the user interface.
Virus Encyclopaedia	Displays the Virus Encyclopedia directly, enabling you to search for details of individual viruses.
Dr Solomon's Anti-Virus Toolkit Help	Displays help information for the Windows NT Toolkit. This is also available from within the Toolkit.

Item	Purpose
Schedule Editor	Enables you to set up scheduled events. See Chapter 6, "Using the Scheduler".
Dr Solomon's Scheduler Help	Displays Help information for using the Scheduler. This is also available from within the Schedule Editor.

To start up the Toolkit, double-click on the Toolkit icon. The following window is displayed:



3.2 The main screen

The main screen provides quick access to the Toolkit's most commonly used functions without having to use the drop-down menus.

The short cuts available are as follows:

Option	Use
To scan for viruses	Select one or more disk drives from the displayed list, then choose Find to scan for any known virus using FindVirus.
To repair infected files and diskette boot sectors	Select a disk drive from the displayed list, then choose Repair to detect viruses and repair files and diskette boot sectors.
To check for changes	The Check for Changes option allows you to perform a check for any changes in executable files, using ViVerify.
Displaying virus information	The Virus Information option lets you browse through the Virus Encyclopedia to find information.

For more information on running these options, see Chapter 4, "Checking for Viruses".

To close the Toolkit, select Exit from the File menu or press Esc.

3.3 Options on the menus

Aside from the short cuts on the main screen, you can select the Toolkit functions from a number of drop-down menus. These are described below.

File menu

The File menu provides options for managing files.

Menu Option	Function
Load Configuration	Lets you load a previously-saved file containing particular Toolkit settings. See Chapter 9, "Toolkit Configuration" for more details.
Save Configuration	Lets you save the current Toolkit settings so that they can be used later. See Chapter 9, "Toolkit Configuration" for more details.
Shred	Deletes a file so that it cannot be recovered. See "Shredding files" on page 52 for more details.
Exit	Exits from the Toolkit.

Scan menu

The Scan menu provides options that enable you to set up and run the virus-checking tools.

Menu Option	Function
Find Viruses	Runs FindVirus, which scans for viruses on any hard disk or diskette.
Check for Changes	Runs ViVerify, which can tell if an executable file has been altered.

Repair menu

The Repair menu provides options that enable you to repair infected files and diskettes.

Menu Option	Function
Repair File	Repairs files.
Replace Boot Sector	Replaces a corrupted boot sector on a diskette with a clean copy.

For more details of these options, see Chapter 5, "Virus Repair and Removal".

Advanced menu

The Advanced menu includes additional options.

Menu Option	Function
Virus Encyclopedia	Lets you view the on-line Virus Encyclopedia and to search for particular information.
Schedule	Allows you to set up schedules to perform events at particular times. See Chapter 6, "Using the Scheduler" for more details.

This page has been left blank

4. Checking for Viruses

This chapter provides a step-by-step explanation of how to run FindVirus and ViVerify from the user interface. For details of how to run the programs from the command line or in batch files, see Chapter 7, "Advanced Virus Detection" and Chapter 8, "Advanced Virus Checking".

4.1 Finding Viruses - FindVirus

FindVirus scans for all the boot sector, partition sector and file viruses listed in the virus driver file. You can use FindVirus to insure that any hard disk or diskette is free from all known viruses.

An option also allows you to run a heuristic analyzer. This technique looks inside files for suspect code combinations that may be a result of new viruses not yet included in the virus driver file.

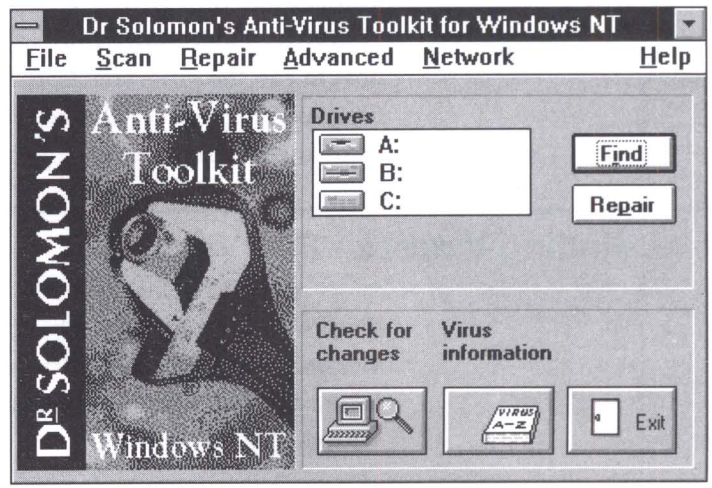
When to use FindVirus

You should use FindVirus to scan all incoming diskettes and files to insure they are free from viruses.

You can also use FindVirus to help clean up a virus outbreak. It will tell you which files are infected, and with what virus. It can also be used to repair the infected files and diskette boot sector viruses.

Running FindVirus from the main screen

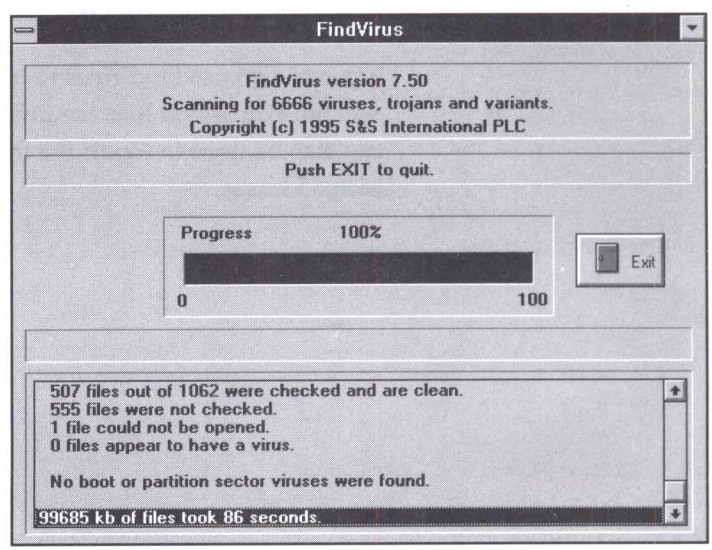
You can run FindVirus from the Toolkit main screen:



Follow these steps:

1. In the Drives box, select the drive(s) you want to check.

2. Select Find. The selected drives are scanned for viruses. When each scan is complete, a report similar to this is displayed:


FindVirus
FindVirus version 7.50
Scanning for 6666 viruses, trojans and variants.
Copyright (c) 1995 S&S International PLC
Push EXIT to quit.
Progress 100%
0 100
Exit
507 files out of 1062 were checked and are clean.
555 files were not checked.
1 file could not be opened.
0 files appear to have a virus.
No boot or partition sector viruses were found.
99685 kb of files took 86 seconds.

3. If you have selected a diskette drive, when the scan is complete you will be asked if you want to scan another diskette. If so, insert the next diskette before choosing Yes.

4. If the logged on username is not in the administrator group FindVirus will not be able to scan the disk's partition and boot sectors, and you will see the messages 'The boot sector cannot be read' and 'The partition sector cannot be read'. In this case you should logon again with a username which is in the administrator group and repeat the scan. If you do not have access to such a username see your System Administrator.

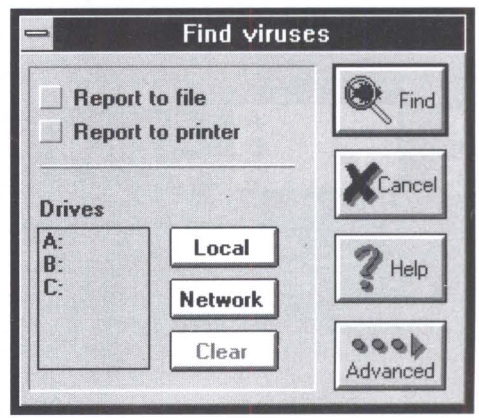
5. If your disk is free from viruses, the message *All clear* is displayed.

If a virus is found, do not panic! See Chapter 5, "Virus Repair and Removal", for information about what to do.

Running FindVirus from the main screen uses the default settings. If you want to change any of these, you need to run FindVirus from the Scan drop-down menu as described in the next section.

Running FindVirus from the Scan menu

1. Select Find Viruses from the Scan menu. The following dialog box is displayed:



2. The settings and options are as follows:

Report to

By default, a report of the scan is displayed on the screen. In addition, you can choose to direct the report to a file, to a printer, or to both.

If you choose Report to file, the report will be saved in a file called FINDVIRU.REP in the TOOLKIT directory. You can change this filename using a setting on the Advanced dialog box.

If you choose Report to printer, the report will be sent to your default system printer. Make sure it is connected, loaded with paper and on line.

Drives

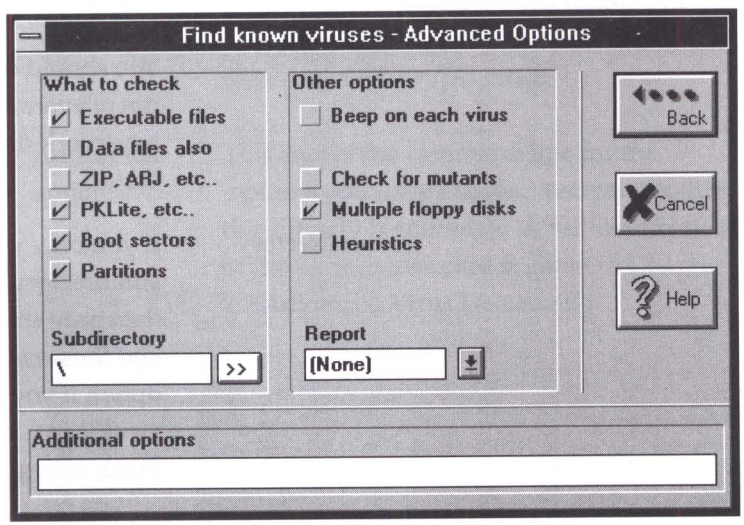
Select the drives you want to scan. Choose Local to scan all the hard drives on your PC. Select Network to scan all network drives. Select Clear to clear any selections you have made.

3. The settings are now suitable for most cases. You can however make additional settings by selecting Advanced - see "Advanced menu options" on page 31 for details.

4. Start the scan by selecting Find or pressing ↵; continue from Step 3 in the section "Running FindVirus from the main screen" on page 28.

Advanced menu options

If you choose Advanced the following dialog box is displayed:



After making the settings select Back to return to the Find viruses dialog box. You can save the settings for future use by selecting Select Save Configuration from the File menu - see "Toolkit Configuration" on page 107 for more information.

The settings and options are as follows:

What to check — By default, FindVirus scans all executable files, boot sectors and partition sectors. You can change these settings if you wish.

Select Data files to scan all non-executable files. Normally, you need only select this option if you are cleaning up after a virus infection.

Select PKZIP, ARJ, ICE, LHA and CRYPTCOM to scan files which have been archived using these formats.

Select PKLite if you want FindVirus to scan files compressed using PKLite, LZExe, LZH and DIET.

You should only deselect Boot sectors if it is not relevant, for example if you are scanning a network drive that doesn't have a boot sector.

Subdirectory

If you only want to scan a particular subdirectory, enter its path here. FindVirus then only scans files in the named directory and those below it. You should only use this option if you are absolutely sure that the virus is in a particular location. It is always much safer to scan the entire drive.

Other options

Select Beep on each virus if you need this extra warning when a virus is found.

Choose Network Alarm on virus to send a message to the network administrator if a virus is found. This option is only visible if your PC is connected to a network.

Choose Check for mutants to scan for mutant viruses, which differ slightly from identified viruses. Setting this option will find these variations, but it increases the chance of a false alarm. It is not necessary for most users.

Choose Multiple floppy disks if you want to scan more than one diskette in the same drive. You are prompted to insert the next diskette when each one has to be scanned.

Choose Heuristic analyzer if you want to run extra checks for potential new viruses. This offers extra protection for users who need more security, but can increase scanning times by approximately 50%.

Report

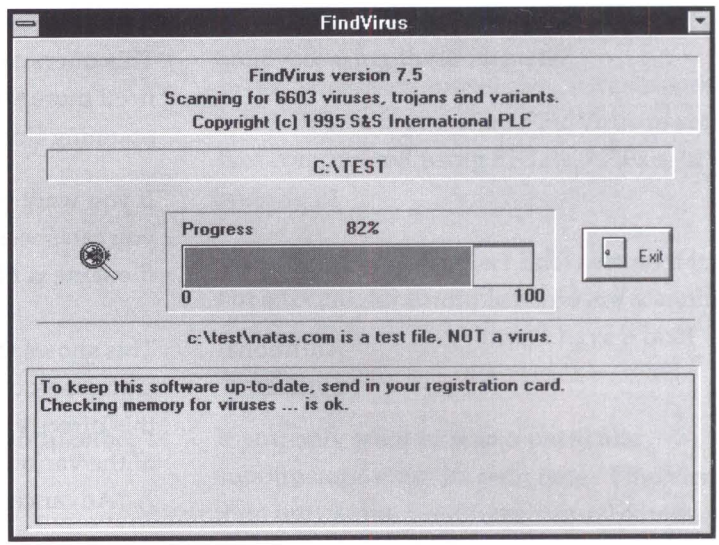
If you want to send the virus report to a file, you can specify a filename here. The default filename is FINDVIRU.REP.

Additional options

This shows the command line for the options you have chosen. You can modify this directly if you wish. A full description of the various switches is given in Chapter 7, "Advanced Virus Detection".

If FindVirus reports a virus

Whenever you run FindVirus, it displays a screen of information. If a virus is found, it sounds an alarm and displays details of the virus similar to this:


FindVirus
FindVirus version 7.5
Scanning for 6603 viruses, trojans and variants.
Copyright (c) 1995 S&S International PLC
C:\TEST
Progress 82%
0
100
Exit
c:\test\natas.com is a test file, NOT a virus.
To keep this software up-to-date, send in your registration card.
Checking memory for viruses ... is ok.

Read the message and make a note of the virus found. Exit in the normal way from whatever you were doing and save any files you were working on.

For details of how to repair the virus infection, see Chapter 5, "Virus Repair and Removal".

4.2 Checking for changes - ViVerify

ViVerify enables you to detect changes in executable files which may be the result of a virus infection. ViVerify works by calculating a unique fingerprint, or checksum, for each file it is protecting. This fingerprint can then be recalculated at any time as a safety check to see if any changes have been made. ViVerify also detects changes in boot and partition sectors.

With this type of tool, you need a balance between speed and security. If the fingerprint calculations are too complex, ViVerify will take a long time to run. On the other hand, if the calculation is too simple, it is possible for a virus to evade detection. This is known as *spoofing*. ViVerify's default settings are a good balance between security and performance. However, you can change the settings if necessary to choose the level of security you want.

ViVerify's default fingerprinting method makes use of a keyword. You have to enter a keyword when the fingerprints are first calculated, and then repeat it every time a check is performed. This increases security by preventing a virus from spoofing the fingerprint.

When to use ViVerify

You can use ViVerify to check executable files regularly.

You can also use ViVerify when cleaning up after a virus infection, as it gives early warning of possible re-infection which can be dealt with before it spreads to other PCs.

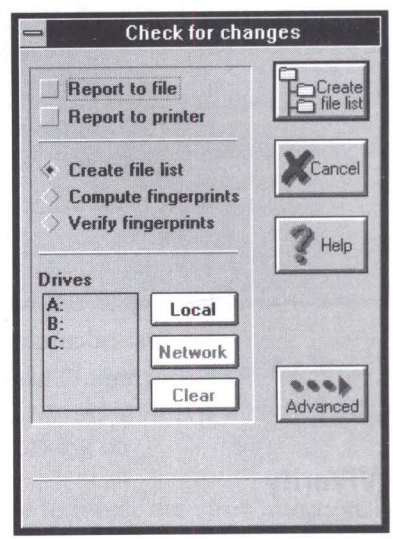
Running ViVerify

You can run ViVerify in two ways:

- From the Toolkit main screen by selecting the Check for Changes box.
- By selecting Check for Changes from the Scan menu.

In both cases the dialog boxes and options are exactly the same.

1. When you select **Check for Changes**, the following dialog box is displayed:



2. The settings and options are as follows:

Report to	A report of the process appears on the screen. In addition, you can direct the report to a file, to a printer, or both. If you select Report to file, the report will be saved in a file called VIVERIFY.REP in the default Toolkit directory. (You can change this filename using an option on the Advanced dialog box.) If you choose Report to printer, the report is sent to your default system printer.

Drives	Select the drives you want to check. Choose Local to scan all the hard drives on your PC. Select Network to check all network drives. Select Clear to clear previous selections.
Keyword	This box only appears when you have selected Compute fingerprints or Verify fingerprints. This is used to encrypt the fingerprints, providing an additional level of protection.

3. These options are sufficient for most situations. Additional options can be specified in the Advanced dialog box.

There are three stages in running ViVerify:

- Firstly, you need to create a list of the files you want to check, using the Create file list option.
- Secondly, you need to calculate the unique fingerprints for each file, using the Compute fingerprints option.
- Thirdly, you can regularly check the set of files for changes, using the Verify fingerprints option.

These three stages are described below.

To create a file list

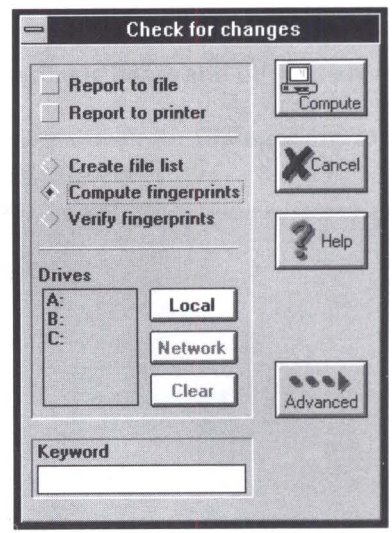
To create a list of files to check:

1. Select Create file list.
2. Select the drives to be checked. For example, select Local to make a list for all local hard disk drives.
3. Press the Create file list button, or press ↵.
4. ViVerify checks the disk for executable files. When the file list has been created, a message is displayed. Press any key (or click the mouse) to return to the main screen.

To compute the fingerprints

To calculate fingerprints for the selected files:

1. Select Compute fingerprints. The dialog box changes slightly:



2. Select the drives to be checked. For example, select Local to make a list for all local hard disk drives.

3. Select the Keyword box. Type in a word of at least eight alphanumeric characters. This keyword is then used as part of the encryption process, which helps prevent a virus from simulating the correct fingerprints.

Note: The keyword is not a password. It is quite safe to write it down and keep it next to the PC - a virus cannot read it!

4. Press the Compute button, or press ↵.

5. When the fingerprints have been calculated, a message is displayed. Press any key (or click the mouse button) to return to the main screen.

Checking the files

Once you have selected the files and computed the fingerprints, you should check them regularly. To check the fingerprints for the selected files:

1. Select Verify fingerprints.
2. Select the drives to be checked. For example, select Local to check the fingerprints for all local hard disk drives.
3. Select the Keyword box. Enter the keyword used previously.
4. Press the Verify button, or press ⏎.
5. When the fingerprints have been verified, a message is displayed. Press any key (or click the mouse button) to return to the main screen.

If a file has changed

If ViVerify indicates that a fingerprinted file has been changed, this does not necessarily mean that you have a virus infection. Other possibilities are:

- The changed files could be data files. Data files will always change when they are modified, and occasionally they have names that make them look like executable files.
- Some EXE and COM files are altered by installation routines.
- If ViVerify reports that all programs have been changed, don't panic. It probably means that you have entered the keyword incorrectly. Check this and run it again before wasting time on an unnecessary clean-up operation.

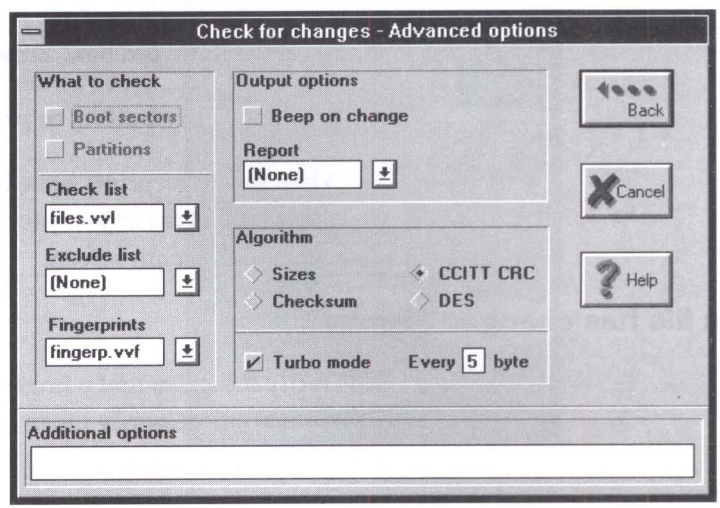
However, if a number of files have changed unexpectedly, it is possible that you have a virus. Make a note of the suspect files, then exit in the normal way from whatever you were doing and save any files you were working on.

Run FindVirus with heuristic checking turned on to check for suspect files. (See "Finding Viruses - FindVirus" on page 27.)

If you have a virus, FindVirus will identify it. Make a note of the details displayed on the report screen. If FindVirus cannot identify a virus in the changed files, it is possible that you have a new virus. See "If you discover a new virus" on page 47.

Advanced menu options

If you select the **Advanced** box from the **Check for Changes** screen, a further screen is displayed:



The settings and options are as follows:

Check list — This identifies the file that contains the list of files to be checked. The default file name is FILES.VVL. The latest version of the file always overwrites the previous one. If you want to check more than one drive in separate runs of the program, you may wish to create a separate list for each drive, for example, C_FILES.VVL. These files are created in the default Toolkit directory unless you specify otherwise.

Exclude list

You can exclude certain files from the checking process if you wish. This parameter identifies the file that holds this list. The default filename is EXCLUDE.VVX. You can add files to this list, or change the filename if you wish. For more details, see Chapter 8, "Advanced Virus Checking".

Fingerprints

The fingerprints created for the files checked are stored in a file called FINGERP.VVF. You can specify a different filename if you wish.

Output

If Beep on change is selected, the PC beeps every time ViVerify finds a changed file.

The Report option is only valid if you have opted to send the checking report to a file. If you want to check more than one drive in separate runs, the latest report will overwrite the previous one. Therefore you may want to create a separate report for each drive, for instance C_VER.REP, D_VER.REP, etc. These files are created in the default Toolkit directory unless you specify otherwise.

Algorithm

This box indicates the method used for calculating the fingerprints. The default calculation method is the CCITT Cyclic Redundancy Check, which is suitable for most users.

The Size algorithm calculates fingerprints based on the file size. This is a very fast calculation, but a few viruses do not change the size of files they infect, and so can evade it.

The Checksum algorithm calculates the fingerprints as a sum of the bytes checked in the files. The keyword is also incorporated.

The DES option calculates the fingerprints using the standard Data Encryption Standard algorithm, incorporating the keyword. This is very secure but requires lengthy calculations. Only use this option if your organization's policy requires this level of security.

More details on encryption methods are given in Chapter 8, "Advanced Virus Checking".

Turbo mode — By default, ViVerify checks just the first and last 4 Kb of each file by default. This speeds up the calculation. It is very unlikely that a virus could infect your system without changing at least one byte in these areas. You can deselect turbo mode if required.

Every n byte — Checking every byte in a file is very time-consuming. By default, ViVerify checks every fifth byte. You can speed up the checking by increasing this number, or increase security by choosing a lower number.

Additional options — This shows the command line for the options you have chosen. You can modify this directly if you wish. Full details of the various parameters and switches are given in Chapter 8 "Advanced Virus Checking".

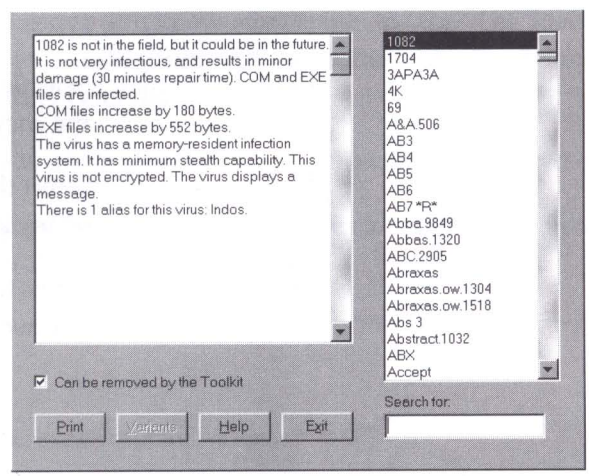
You can save the changed ViVerify settings for future use. Select Save Configuration from the File menu. For more information, see Chapter 9, "Toolkit Configuration".

4.3 The Virus Encyclopedia

The on-line Virus Encyclopedia contains details of all the viruses recognized by FindVirus. You can view the Encyclopedia in two ways:

- From the Toolkit main screen by selecting the Virus Information button.
- By selecting Virus Encyclopedia from the Advanced drop-down menu.

The following screen is displayed:



You can look at information about a particular virus by selecting it from the list. You can scan through the list using the scrollbars.

For each virus, the Encyclopedia gives the following information:

- How common it is.
- How infectious it is.
- How much damage it does.

- What is infected: files, boot sectors or partition sectors.
- Whether or not it has memory-resident capabilities.
- If it uses stealth.
- If it is polymorphic.
- Any aliases it is known by, and whether there are any variants.

There are a number of options available from this screen.

Search	To find out information about a particular virus, move to the Search box and type its name. You do not need to press ↵, just type in the characters.
Help	Selecting Help displays information about the encyclopedia and how to use it.
Variants	Select the Variants box to display the names of any known variants.
Print	Prints the displayed information about the selected virus.

5. Virus Repair and Removal

This chapter explains the steps you need to follow to remove viruses and carry out repairs to executable files, boot sectors and partition sectors.

It also suggests a strategy for dealing with a major virus outbreak.

If you have discovered a virus:

- Don't panic. More damage is caused by people attempting to repair the problem wrongly than by viruses themselves.
- Make sure you know what action to take. The Toolkit provides straightforward repair methods. Read through this chapter carefully.
- If you are in any doubt, leave the computer turned off.
- If your company has procedures for dealing with viruses, you should follow them.

5.1 If you find a Virus

Are you sure you have a virus?

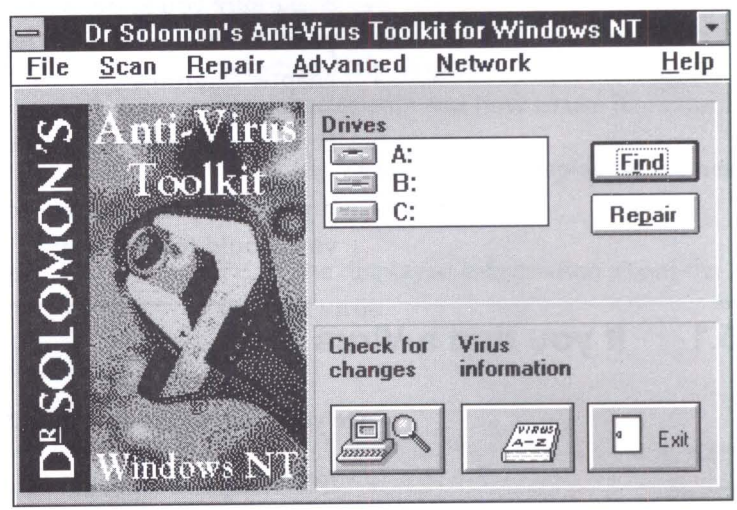
- If ViVerify has reported suspect files, this does not necessarily mean you have a virus. Run FindVirus with heuristic scanning on to check suspect files. If you have a virus, FindVirus will identify it. See "Finding Viruses - FindVirus" on page 27.
- If FindVirus reports a named file virus or a diskette boot sector virus, you can repair it easily with the Windows NT Toolkit. See "Single button repair" on page 46.
- If FindVirus reports suspect files, but does not name a virus, you may have a new virus. See "If you discover a new virus" on page 47.

- If FindVirus finds a virus in the boot or partition sector of a hard disk, you cannot repair it using the Windows NT Toolkit. You need to reboot the system under DOS and run the DOS Toolkit. See separate documentation for full details. If you are in any doubt, contact S&S Support staff. See "If you need help" on page xii.

5.2 Single button repair

The Toolkit includes a straightforward facility for repairing infected files and diskette boot sectors.

The single-button repair can be run from the main screen:



In the Drives box, select the drive on which you have found a virus, then select Repair.

The repair program operates as follows:

1. Any infected files are repaired, if possible. If a file cannot be repaired, it is renamed. The first character of each file extension is changed to a V. For example COM is changed to VOM and EXE to VXE.

2. If the boot sector of a diskette is infected, it is replaced with a clean boot sector.

The Repair program cannot repair infected boot sectors or partition sectors on hard disks. You need to reboot your system under DOS and run the DOS FINDVIRU.EXE executable with the `FINDVIRU/REPAIR` switch at the command line. DO NOT do this however if there is a possibility that an infected NTFS boot or partition sector may be found. If FindVirus tries to repair such a partition sector the data is likely to become corrupted. If a virus is reported in an NTFS boot or partition sector contact S&S for advice.

When the repair is complete, it is recommended that you run FindVirus again to confirm that the disk is free from viruses.

5.3 If you discover a new virus

You may have discovered a new virus in the following situations:

- If you have run FindVirus with heuristic scanning switched on and suspect files have been found.
- If ViVerify notifies you of a changed file, but FindVirus does not find a recognized virus.

If you suspect a new virus:

1. Boot normally and format a diskette in the infected computer.
2. Copy any files that you suspect are infected to the diskette.
3. Copy the following additional files to the diskette:

   MEM.EXE
   TREE.COM

CHKDSK.COM
DISKCOPY.COM
MODE.COM

Run each of these programs from the diskette.

4. Contact S&S Technical Support directly, or your authorized distributor.

5. Do not run anything on the infected PC. If the PC is attached to a network, disconnect it to prevent other users from accessing any files.

S&S can tell you whether the problem is a virus or not, and what you need to do. See "If you need help" on page xii.

5.4 Repair menu options

As an alternative to the Repair button, you can repair files and diskettes from the Repair menu.

Repairing files

You can repair infected files using the Repair files option on the Repair menu. This runs FindVirus to find and repair viruses. The following screen is displayed:

The settings and options are as follows:

Report to	A report of the repair process is normally displayed on the screen. In addition, you can direct the report to a file, to a printer, or both.
Drives	Select the drives you want to scan. Choose Local to scan all the hard drives on your PC. Select Network to scan all network drives. Select Clear to clear any selections you have made.
If file is not repairable	By default, if a file cannot be repaired, FindVirus renames it to prevent someone from running it accidentally. The first letter of the file extension is changed to a V. For example, FORMAT.COM is changed to FORMAT.VOM. If you set the Delete infected files option, FindVirus will delete any files that cannot be repaired.

Files are overwritten before deletion to insure that they cannot be recovered by an Undelete program.

When all the settings are correct, select Repair. FindVirus scans the specified drives and attempts to repair any infected files.

Note that when FindVirus is run with the Repair option it scans all files, including data files. This is in case an executable file has been renamed with a different file extension. It also scans files that have been compressed using PKZIP, PKARC, PKLite, DIET, ICE, ARJ, LZExe, LZH and CRYPTCOM.

FindVirus produces a report detailing the action taken. If any files cannot be repaired, you must restore the original clean copies from backups.

Replacing diskette boot sectors

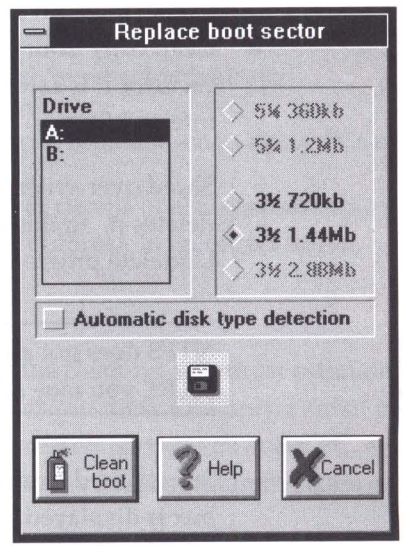
You can replace an infected boot sector on a diskette with a valid, non-infected boot sector using the Replace boot sector option on the Repair menu.

The single-button repair facility will also replace diskette boot sectors. See "Single button repair" on page 46.

This tool does not delete the boot sector virus, but simply overwrites the entire boot sector so that the diskette is no longer infected.

Replace boot sector works on 5¼" diskettes of 360 Kb and 1.2Mb capacity, and on 3½" diskettes of 720 Kb, 1.44 Mb and 2.88 Mb capacity.

Place the diskette you want to repair in the drive and select Replace boot sector from the Repair drop-down menu. The following screen is displayed:



The system automatically detects the number and type of diskette drives on the PC. Select the appropriate drive in the Drive box.

Select the size and capacity of the diskette to be repaired. If you are not sure of the diskette capacity, select Automatic disk type detection. The system then checks the diskette type itself.

Select OK to replace the boot sector.

If the virus has made other changes to the diskette, apart from overwriting the boot sector, these will not be undone by running Replace boot sector. For example, if the virus has created fake bad sectors to store part of itself, those bad sectors will still be there. However, the diskette is safe to use, as code in those sectors can no longer be executed.

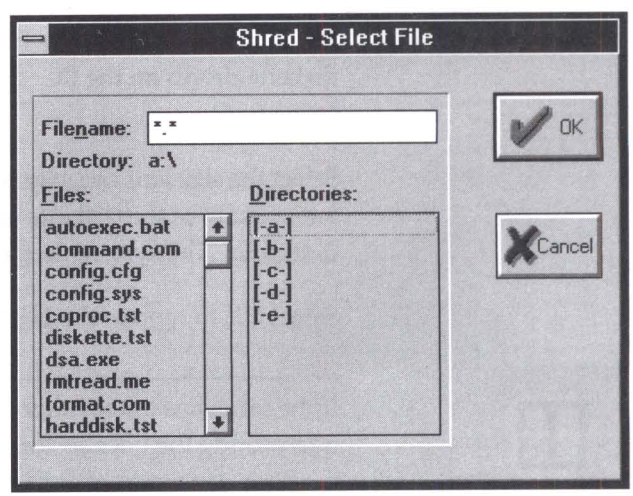
5.5 Shredding files

If FindVirus has been unable to repair an infected file, and has changed the first letter of the file extension, you should restore a clean copy from backup and delete the renamed file. To insure security, it is safer to use the Shred program to delete those infected files.

Shred overwrites a file with a series of characters, and then deletes it. In this way the file cannot be recovered using an Undelete program.

NTFS does not allow undeleting. However, if you do not use NTFS, you may still require this tool.

Select Shred from the File menu. The following file selection box is displayed:



Select the file to be shredded, and select OK. You are asked to confirm the action, since you are not able to restore the file. The file is overwritten and then deleted.

5.6 Eradicating a virus

If you have a major virus outbreak in your organization, it is essential that you find and clean up all the infected systems and media. If you leave out just one diskette or workstation, you will soon be back to where you started.

This is not a trivial problem when many PCs are involved.

This section gives details of a suggested strategy for cleaning up after a virus outbreak in an organization.

Planning the clean-up

Before starting the clean-up you must estimate the size of the problem. Even if you think that only a small percentage of PCs are infected, it is essential to check every PC, every diskette, and all other data storage media within the company.

You must either visit all user areas and check the media in situ, or collect all the diskettes into a central checking location. In the latter case you will also have to insure that all diskettes are returned to their rightful owners.

Firstly you should estimate how many PCs and how many diskettes need to be checked. You can then work out how many people you will need and how long the operation will take. On average, you can assume 50 diskettes per computer, with a maximum of 100 and a minimum of 25.

Unless your organization is very small, it is best to do the clean-up over a weekend, so normal work is disrupted as little as possible.

You will need several PCs to scan the diskettes. Make sure you have 3½" and 5¼" drives if you use both types of diskette. Obviously, you need to make sure the PCs used for checking are clean first!

If there are several thousand diskettes to be checked, it may be worthwhile renting or buying a diskette autoloader. A special version of the Toolkit is available which will run on a PC connected to an autoloader. For more information, call S&S or your authorized distributor.

Once you know the size of the task, you can organize the staff you need. One person should always be designated the diskette controller, with responsibility for all incoming and outgoing diskettes. As an example, for an organization with 20 computers, you would need:

Job function	Number required
Operations controller/ technical advisor	1
Diskette controllers	1
Hard disk team	1
Diskette checkers	3, or 1 if an autoloader is used.

An organization with 200 computers and 20,000 diskettes will need the following people:

Job function	Number required
Operations controller/ technical adviser	1 plus assistant.
Diskette controllers	1 plus assistant.
Hard disk team	3
Diskette checkers	6, or 2 if an autoloader is used.

You will need the willing co-operation of the users, otherwise they won't turn in all their diskettes and backups. Consider allowing users to send in PCs and diskettes from home as well.

Ask all PC users to pack up their diskettes, and send them to the diskette controller on the Friday evening.

Checking diskettes

Start early on Saturday morning and start up the autoloader as soon as possible. If you keep the autoloader running continuously, it should check about 700 diskettes an hour.

The diskette controller should have a large box of diskettes ready to start feeding through. Deal with all the diskettes from each user in one batch. Once this has been set in motion, the rest of the clean-up operation can be started.

The diskette controller's job is to issue diskettes to the checkers and receive them back, checking that the quantity is the same, and that they have all been checked. In a big clean-up there will be at least two controllers, one for diskettes coming in and one for those going out.

One person should be in be charge of the autoloader, keeping it fed with diskettes, and restarting it if it jams or empties. Swap duties if necessary so that people can have breaks, but try and keep the autoloader running.

Any diskettes failed by the autoloader should be passed to a second workstation for manual checking.

Any diskettes that are unreadable should be marked as "NOT CHECKED" and the user advised to reformat them as soon as possible.

If the diskettes are readable, run FindVirus to scan for viruses and then run the Repair options to repair infected files and sectors. If there is any uncertainty, the diskette should be put aside for a final check by Operations Control.

Diskettes which pass the final check should be returned to the diskette controller for return to the user. All checked diskettes should be write-protected, and marked to show that they are

clean. This will give users confidence that their diskettes have been checked.

Checking PCs

While the diskettes are being checked, other staff can be checking the hard disks of PCs. If PCs have been sent to the clean-up room you can use the same keyboard, power cables and screen for each machine. If the PCs need unpacking and assembling, set up a production line to do so.

Follow the same procedure for all the PCs in the user areas. While the software is running check for any diskettes that haven't been handed in. Users may have overlooked backups, or diskettes that are thought to be blank. Any diskettes found should be sent to the diskette controller.

By about 5 pm on Saturday you should have a good idea how the job is going. Make plans for the next day and make arrangements for any staff that have to work late.

When the operation is complete, you should be left with a relatively small number of infected diskettes. These are generally easily dealt with by doing a file-by-file copy from one diskette to another, in the case of boot sector viruses, or by deleting the file in the case of file viruses.

By Monday morning you should have a clean building. Tell users how it went over the weekend, and explain the precautions that have been installed to prevent a recurrence.

6. Using the Scheduler

This chapter explains how to use the Scheduler which is provided in the Anti-Virus Toolkit for Windows NT. This facility allows you to scan your hard disks for viruses, using FindVirus, at any time, even while your PC is unattended. You can also use the Scheduler to run any application on a regular basis, and to send messages to any other users on your network.

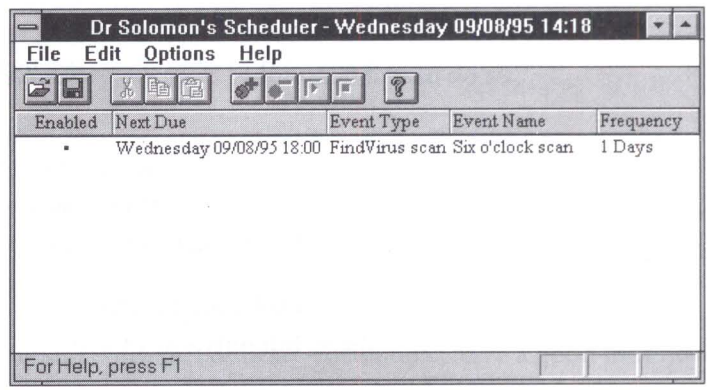
To use the Scheduler, you need to use the Schedule Editor to create an event detailing the program to be run and the time details. Then start the Dr. Solomon's Scheduler service.

Events are stored in event files. You can create any number of these, but only one of them will be active at any one time.

You can set an event once, at a pre-determined time, or you can run it at regular intervals. For example, you can run FindVirus every week to search your hard disks. Details of events performed can be written to a log file, so you can check the results.

6.1 The Schedule Editor

To check the current schedule, select Schedule Editor directly from the Anti-Virus Toolkit program group. A screen of the following format is displayed:



This screen summarizes any events you have already set up. The Enabled column indicates whether or not this event is scheduled to run.

To create new events or modify existing events, you can either choose options from the drop-down menus or click on items on the toolbar running along the top of the screen. The toolbar icons are as follows:

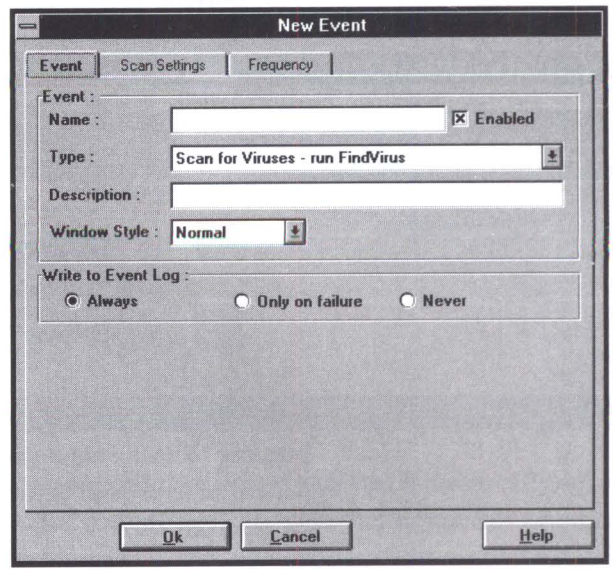
Toolbar icon	Purpose
	Cut selected text and place on clipboard.
	Copy selected text to the clipboard.
	Paste text from the clipboard.
	Open previously saved event file.

Toolbar icon	Purpose
	Save current event file.
	Add new scheduled event.
	Delete highlighted event.
	Enable highlighted event.
	Disable highlighted event.
	Display Help information about the Scheduler.

If the Tooltips option is switched on, a box explaining the purpose of each icon appears when you move the cursor to a particular icon (see "Setting up Scheduler defaults and options" on page 68).

6.2 To set up a new event

Select Add New Event from the Edit menu, or select the Add Event icon. The following screen appears:



The three tabs at the top of the screen let you to set up the event.

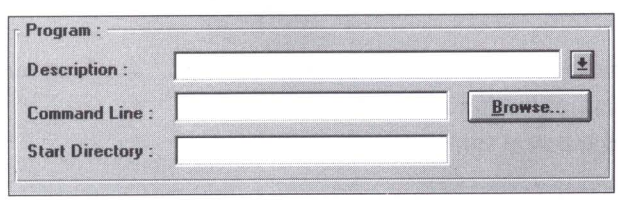
Event	Lets you to set up details of the event to be scheduled.
Scan settings	Lets you to specify details of the virus checks to be carried out.
Frequency	Lets you specify the frequency of the event.

Setting the event details

On the Event screen, the settings and options are as follows:

Name	Identify the new event. The Name appears on the schedule and the event log, so make sure it identifies the event and is unique.
Enabled	Select Enabled to insure the event is run. Clear Enabled to prevent the event from running
Type	Choose the type of event to be performed - Scan for Viruses, Run an Application or Send a Message.
Description	Enter some explanatory text, if you wish.
Window style	Choose how the relevant window is to appear when the event runs - normal, maximized, minimized or hidden.
Write to event log	Choose whether or not to record details of the event in the Toolkit log file. You can record all events or just those that fail.

If you choose Run an Application some additional information is displayed at the bottom of the Events screen:



Description	Select the program to be run from the drop-down list, if you have already set it up as a default. See "Setting up Scheduler defaults and options" on page 68. Alternatively, you can enter a Description directly.

The Command Line and Start Directory will appear automatically if you have chosen a default. Otherwise, press Browse to find and select the program.

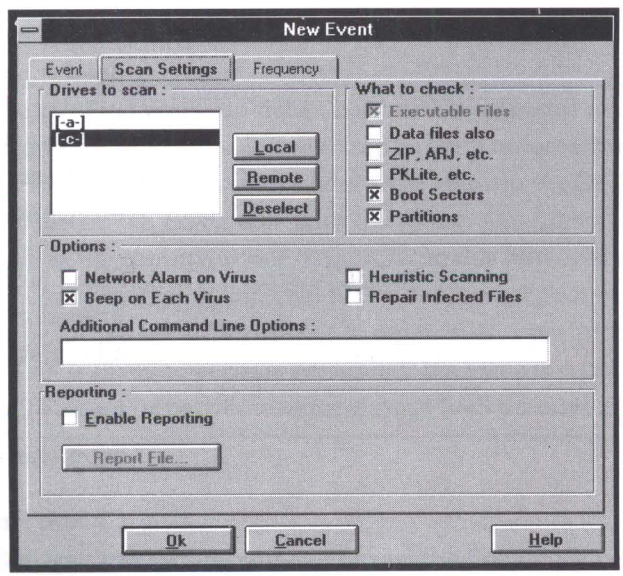
If you choose Send a Message, some additional information appears at the bottom of the screen:

Message — Type in the message you want to send. Alternatively, if you have already set it up as a default, you can select the message from the drop-down list. See "Setting up Scheduler defaults and options" on page 68.

Send to — Choose the user to whom you want to send a message, or select Screen to display the message on the screen.

Scan settings

If you are scheduling FindVirus, you need to choose the Scan Settings tab. (This tab is not available when scheduling other events.)



The settings and options for FindVirus are as follows:

Drives to scan — Choose Local to scan all the drives on your PC. Choose Remote to scan all the remote drives. Press Deselect to remove a selection.

What to check — By default, FindVirus scans all executable files, boot sectors and partition sectors. You can change these settings if you wish.

Select Data files also to scan all non-executable files.

Select ZIP, ARJ to scan files which have been archived using these and other formats.

Select PKLite if you want FindVirus to scan files compressed using PKLite, ICE, DIET, LZH and LZExe.

You should only deselect Boot sectors if this causes a particular problem; for example, if you are scanning a network drive that doesn't have a boot sector.

You should only deselect Partitions to suppress partition sector scanning when this causes a problem.

Options

Select Network Alarm on Virus if you want to send a warning message to the network administrator if a virus is found.

Select Beep on Each Virus if you need this extra warning when a virus is found.

Choose Heuristic Scanning if you want to run extra checks for potential new viruses. This offers extra protection for users who need more security, but can increase scanning times by approximately 50%.

Choose Repair Infected Files if you would like any infected files to be repaired automatically.

Reporting

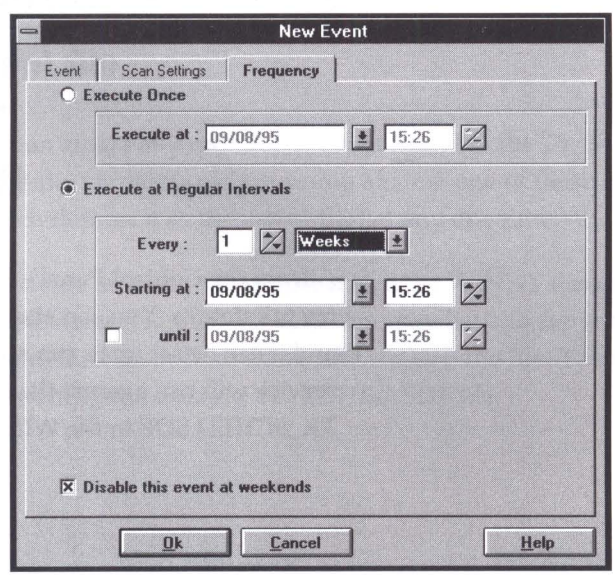
Select Reporting if you want a report file to be generated. Select Report File to choose or create a filename.You can include the full UNC path to a remote server share, but you must make sure the parent user ID has permission to write to it. It is recommended that you set up a low access user ID for the entire network which can be read everywhere (for scans), but which can only write to the user share. To help create unique report filenames you can use two

string substitutions: where you include %HOST in the filename you enter here, you will see the hostname in the generated report file's name, similarly %UCT is substituted by a hexadecimal representation of the time of the report.

Although FindVirus can detect hard disk boot sector and partition sector viruses, it cannot repair them automatically. You need to reboot your system under DOS and run the DOS FINDVIRU.EXE executable with the `FINDVIRU/REPAIR` switch at the command line. DO NOT do this however if there is a possibility that an infected NTFS boot or partition sector may be found. If FindVirus tries to repair such a partition sector the data is likely to become corrupted. If a virus is reported in an NTFS boot or partition sector contact S&S for advice.

Frequency settings

For all types of events, you need to set the Frequency options.



If you only want to run the event once, select Execute Once. Then enter the date and time that the event is to be run.

If you want to run the event on a regular basis, select Execute at Regular Intervals. Enter the frequency, for example, Every 2 Days or Every 4 Weeks. Enter the date and time that you want the event to start. If you wish, you can also enter an end date and time.

If the event is only to run on weekdays, select Disable this event at weekends.

You can type dates and times directly, or you can use the Windows buttons to change the default entries.

6.3 Starting and stopping the Scheduler

Once you have set up regular events, you need to consider the running of the Scheduler.

The Scheduler is implemented as the 'Dr. Solomon's Scheduler' service. You control the running of services by selecting Services...

... from the Control Panel - see your Windows documentation for full details. You can start or stop the scheduler at any time, and it can be set up to run automatically on system startup. The service will run against the event file with the name TK_SCHED.SDF in the WINNT directory.

6.4 Managing an event file

You can use the standard Windows cut and paste functions to copy details of existing events.

To edit an event after you have set it up, either highlight it in the event list and select Edit Event from the Edit menu or simply double-click on the event.

If you want to temporarily prevent an event from running, select the Disable icon (or clear the Enable check box on the Event screen). To resume it, click the Enable button.

Event files can be edited with a text editor - after doing this you can run Validate from the File menu to check the syntax and delete any invalid entries directly. Event files may have any name, however the active event file is stored as TK_SCHED.SDF in the WINNT directory.

The options for saving the event file depend on the defaults set up. See "General defaults" on page 69 for details.

6.5 Activating an event file

You can create any number of event files, but the Dr. Solomon's scheduler service is only running against one of these files (which defines it as the active file) at any one time.

To activate an event file ensure it is in the WINNT directory and has the name TK_SCHED.SDF. You may have to move the file, rename the file, or both move and rename the file. You will be overwriting the existing TK_SCHED.SDF file.

6.6 The Toolkit Event Log

Depending on the settings you have included on the event screen, information may be written to the log file whenever an event is performed, or when an event fails to run.

To check the log file, select Event Log file from the File menu, then choose View. This will run Windows Notepad with the log file loaded so you can check the event.

By default, the log file is saved as TK_SCHED.LOG in the WINNT35 directory. You can change the name and path if you wish, by selecting Event Log file from the File menu, then Change Name.

6.7 Setting up Scheduler defaults and options

The Options menu lets you choose how the Scheduler screens appear and what the standard settings are.

The Font option lets you change the typeface and size used when the event file is displayed.

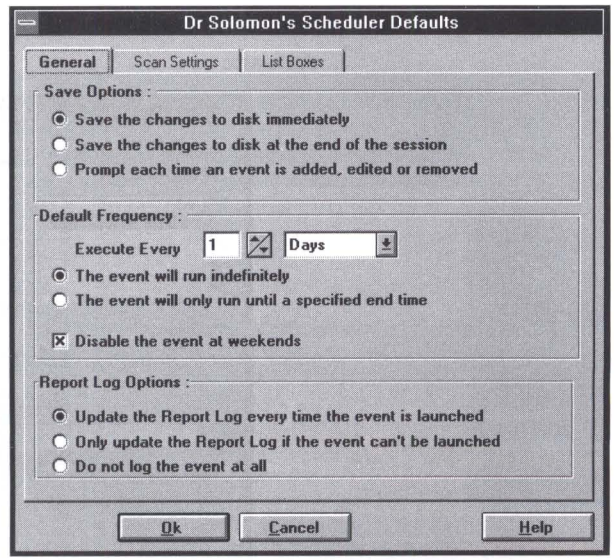
If you select Show Toolbar, the toolbar appears at the top of the screen. This offers an alternative way of choosing the options.

If you select Show Status Bar, the status bar at the bottom of the screen appears.

If you select Show Tooltips, a box explaining the purpose of each icon appears when you move the cursor to a particular icon.

The Defaults option on the Options menu allows you to set the default values for the various Scheduler screens.

If you choose this option, the following screen appears:


Dr Solomon's Scheduler Defaults
General
Scan Settings
List Boxes
Save Options :
Save the changes to disk immediately
Save the changes to disk at the end of the session
Prompt each time an event is added, edited or removed
Default Frequency :
Execute Every
1
Days
The event will run indefinitely
The event will only run until a specified end time
Disable the event at weekends
Report Log Options :
Update the Report Log every time the event is launched
Only update the Report Log if the event can't be launched
Do not log the event at all
Ok
Cancel
Help

The three tabs at the top of the screen let you select the various categories of defaults. Select OK when you have finished.

General defaults

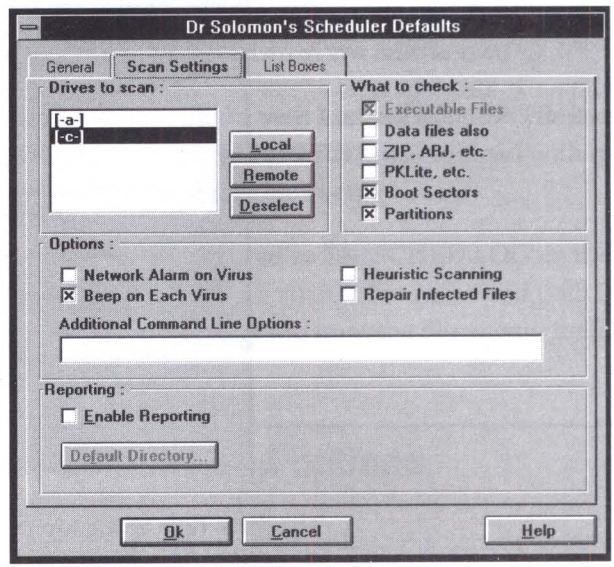
On the General defaults screen the settings are as follows:

Save Options	Choose whether changes to the event file should be saved straight away, when you have finished using the Schedule Editor, or whether a prompt should be issued whenever a change is made.
Default Frequency	Set up the default values that will appear on the Frequency screen.
Report Log Options	Set up the default for writing events to the event log.

Remember these are the default values that appear on the screen when you set up new events. You can always change them to suit your individual requirements.

Scan Settings

If you choose the Scan Settings tab, the following screen appears:

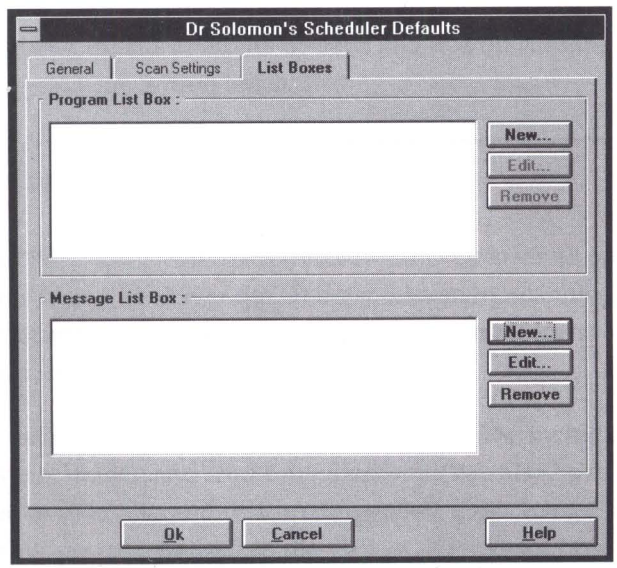


Set up the FindVirus settings that you are most likely to use. The settings are described in "Scan settings" on page 63.

Remember these are the default values that appear on the screen when you set up new events. You can always change them to suit your individual requirements.

List Boxes

If you choose the List Boxes tab the following screen appears:



This allows you to set up frequently-run programs and commonly-used messages that can then be selected from drop-down lists on the Event screen.

In the Program List Box, select the New button to choose a new application program to add. All available programs are listed, and you can browse through and pick the one that you want.

In the Message List box, select New to enter a new message.

In both boxes you can edit or delete existing entries by highlighting the entry and choosing the appropriate button.

This page has been left blank

7. Advanced Virus Detection

This chapter includes technical information on using FindVirus, including details of all the options and tips on running the program from within batch files.

7.1 How FindVirus works

FindVirus scans your hard disks and diskettes for all the viruses listed in a virus driver file. It detects them by scanning the files for recognizable strings of bytes from within the virus code, and other sophisticated methods.

By default, FindVirus scans all executable files, including system, hidden and read-only files, but it can also be configured to scan data files and inside compressed files. Long filenames are supported. As well as file viruses, it looks for boot sector viruses and partition sector viruses. FindVirus also finds common trojans and jokes.

FindVirus has been optimized for virus scanning, so it works very quickly. For example, an 80 Mb hard disk full of executable files can be scanned in about 20 seconds. Obviously, the faster the PC, the faster FindVirus works.

FindVirus can be run from the Scan drop-down menu, or directly from the main screen by selecting Find. Details of using it in this way are given in Chapter 4, "Checking for Viruses".

Because it scans for the viruses listed in the driver file, it is vital that the file is kept up-to-date. If your version is out-of-date, a message is displayed to that effect when you run FindVirus. See "Registration and upgrades" on page xi.

Executable files

File viruses only infect executable files; these may include some data files containing executable macros. By default, FindVirus scans for files with the following extensions:

APP	DOT
BAT	EXE
BIN	OV?
CMD	QLB
COM	SYS
DEV	XTP
DLL	001
DOC	002

If you have executable files with other extensions, you should set FindVirus up to scan for all files. In its default mode, FindVirus scans every executable file in every subdirectory on a disk.

Compressed and archived files

FindVirus can scan for viruses in files that have been compressed using many common archiving programs. It achieves this by decompressing as much of the files to memory as necessary and then scanning them for viruses. Because the PC's available memory is used to decompress files, it does not need any hard disk space or access to diskettes. FindVirus can scan files compressed using the following tools:

PKLite	ARJ
DIET	ICE
LZH	LZExe
PKZIP	

Others will be added in future releases.

By default, scanning of compressed files is turned off.

FindVirus can also scan inside "unextractable" PKLited files.

Self-extracting archived files, such as those created with the PKWare utility ZIP2EXE, can also be scanned. FindVirus also supports multi-disk archives.

If you have multiple-level archived files, such as ARJ files within ZIP files, FindVirus recursively decompresses all levels and scans them completely for viruses if enough memory is available.

When scanning compressed executable files, FindVirus reports that it has scanned the self-extractor code and then that it has scanned the contents of the compressed file. This does not mean that the same file is scanned twice.

If you have ZIP or ARJ files that have been encrypted with passwords, FindVirus is unable to scan them for viruses. In these instances it displays a message at the end of the scan warning that password-encrypted files were found and have not been scanned. For complete security you should unpack these files manually and decrypt them before scanning them.

Scanning compressed and archived files slows down FindVirus and is really only necessary for sheep-dip PCs.

Repairing files

FindVirus can also be run with the Repair option, to remove viruses and repair the files most susceptible to virus infection. It attempts to remove any viruses and restore the files.

For more information, see Chapter 5, "Virus Repair and Removal".

7.2 Running FindVirus from the user interface

You can run FindVirus from the user interface in the following ways:

- From the main screen, by choosing the drives to be scanned and selecting Find.
- By selecting Find Viruses from the Scan menu.

These options are explained in detail in Chapter 4, "Checking for Viruses".

7.3 Running FindVirus from the command line

You can run FindVirus directly from the command line by selecting Run from the File menu within Program Manager. You can also include the appropriate commands within a batch file.

Syntax

The command syntax is:

```
WFINDV32 [switches]
```

The switches are as follows:

Switch	Meaning
/ALLDRIVES	Scan all fixed disk drives, including network drives.
/ANALYZE	Run heuristic analyzer, to look for possible new viruses.
/BADLIST=*file*	Write suspect filenames to the specified file.
/BEEP	Beep when a virus is found.
/CHECKLIST=*file*	Scan files listed in specified file.

Switch	Meaning
/D=drives	Scan specified drives.
/D=drives	Scan specified drives.
/DISINFECT	Scan executable files and attempt to repair infected ones. If a file cannot be repaired it will be renamed and its file permissions set to prevent access by users without administrator privileges.
/DISINFECT /MOVE[=*path*]	Backs up files to the directory specified before a repair is attempted. If the infected file cannot be repaired the original is deleted.
/DRIVER=*file*	Use named virus driver file.
/EVLOG	Report FindVirus activity to the NT event log. Scans create entries under the 'FindVirus' category, scans which find an infection also create an entry under the 'Infection' category.
/EXTERROR	Provide extended error levels.
/EXTRA=*file*	Use named additional virus driver.
/FORCEFLOPPY	Force reading of diskette boot sector when diskette is changed.
/HELP /?	Display the most common FindVirus switches.
/INI	Read parameters from INI file
/LOCAL	Check local hard disk drives.
/LOUD	Display status of each file scanned.

Switch	Meaning
/MOVE	The directory CONFINED.VIR is created and when an infected file is found it is inserted in the path between the root of the file's volume and the rest of the path. If the attempt to move the file fails it is renamed its file permissions set to prevent access by users without administrator privileges.
/MOVE=path	The specified directory is created (if it doesn't already exist) and inserted at the top of the path of any infected files found. If a drive is not specified the directory is created in the root of the infected file's drive.
/MSG=*message*	Send message to the network administrator.
/MUTANT	Search for mutant viruses.
/NOBOOT	Do not scan boot or partition sector.
/NOFILES	Disable file scanning.
/NOMSG	Disable network broadcast.
/NOPACK	Do not scan files compressed with PKLite and LZExe.
/NOPART	Do not check partition sectors.
/ONEONLY	Check one diskette only.
/ONVIRUS="*msg*"	Display the specified message if a virus is found.
/PACK	Scan files compressed with PKLite and LZExe.
/PAUSE	Pause for keystroke before scanning.
/PRINTOUT	Output report to the printer as well as to the screen.

Switch	Meaning
/QUEUE=*print-queue*	The report is sent to the specified print queue.
/REPAIR	Scan all files (as if the /DOALLFILES switch had been specified) and attempts to repair infected files. If a file cannot be repaired it is renamed and its file permissions set to prevent acccess by users without administrator privileges.
/REPAIR[/DELETE]	As for /REPAIR but the optional /DELETE switch deletes files that cannot be repaired.
/REPORT=*file*	Output report to specified file.
/SILENT	Suppress screen output.
/SUMMARY	Produce a summary report.
/TELL=*name*	Send network messages to user.
/UNPACK	Scan compressed files. (Superseded by /UNZIP and /PACK.)
/UNZIP	Scan files compressed with PKZIP, ARJ, PKLite, LZExe, ICE ,DIET, LZH, PKARC, and CRYPTCOM.
/YESBREAK	Enable interruption with Ctrl Break.

The action of the switches is discussed in the following sections. You cannot use any switch more than once on the command line. For example, only the first /LOCAL has any effect. The switches must be separated by spaces and can be in upper or lower case. You can display the most common switches by running WFINDV32 with the /? or /HELP switches.

Scanning specific drives

The most common way of defining the drive to be scanned is to specify the drive on the command line. For example, to scan the C: drive, use:

```
WFINDV32 C:
```

Alternatively, you can use one of the following switches:

```
/D=
/ALLDRIVES
/LOCAL
```

If you do not specify a drive, FindVirus prompts for the drive to be scanned.

The `/D=` switch allows you to specify one or more specific drives.

`/D=`*`drive`* Scans the specified drive(s).

For each drive you want to scan, enter the identifying letters, without spaces between them. You do not need to enter the colon. For example:

```
WFINDV32 /D=CD
```

scans the C: and D: drives.

`/ALLDRIVES` Scans all fixed disk drives, including network drives.

`/LOCAL` Scans the current local hard disk drives.

If you specify a diskette drive, FindVirus will automatically scan a number of diskettes in the same drive. For example:

```
WFINDV32 /D=A
```

Once each diskette has been scanned, you will be prompted to remove it and insert the next. You can change this default with the following switches:

`/ONEONLY` Scans one diskette only, and does not prompt for further diskettes.

`/PAUSE` Pauses after loading a diskette.

For example:

```
WFINDV32 /D=A /ONEONLY
```

scans just one diskette in drive A:, and does not prompt for further diskettes.

Scanning files and subdirectories

By default, FindVirus scans all executable files on the specified drive. You can modify this with a number of switches.

You can specify a directory to be scanned on the command line. For example:

```
WFINDV32 C:\USERS\FRED
```

To scan data files as well as executables, use the `/DOALLFILES` switch. For example:

```
WFINDV32 /LOCAL /DOALLFILES
```

scans all files (executable and data) on the local hard drive.

You can specify a single file or list of files to be scanned on the command line. For example:

WFINDV32 FILE.TXT

or `WFINDV32 FILE1.TXT, FILE2.TXT`

You can also use the `/CHECKLIST` option:

`/CHECKLIST=`*`file`* Scans only the files listed in the specified file.

You can create a file containing the names of the files you want FindVirus to scan using a text editor or word processor. This

must be an ASCII file containing only the filenames, including extensions, one filename on each line. Do not include drive or path specifiers.

You can also use this option to scan suspect files included in a list produced by ViVerify with the `/BADLIST` option. See "Producing a list of suspect files" on page 105.

For example:

```
WFINDV32 /CHECKLIST=SUSPECT.LST
```

scans just those files listed in SUSPECT.LST. If a pathname is not given, the file is assumed to be in the default Toolkit directory.

Scanning network shares

You can specify network shares to be scanned using UNC (Universal Naming Convention) filenames, for example:

```
WFINDV32 \\ACCOUNTS\PUBLIC
```

scans the PUBLIC share on the server named ACCOUNTS.

Scanning compressed files

By default, FindVirus does not scan any compressed and archived files. If you want to scan these files, use the `/UNZIP` and `/PACK` options.

`/PACK`	Scans files that have been compressed using the PKLite and LZExe utilities.
`/UNZIP`	Scans files that have been archived or compressed with PKZIP, PKLite, LZExe, ARJ, ICE, LZH, PKARC, CRYPRCOM and DIET utilities.
`/NOPACK`	Turns off scanning compressed files (PKLite and LZExe). This is the default setting.

For example:

```
WFINDV32 C: /NOPACK /UNZIP
```

enables the scanning of archived files (such as PKZIP and ARJ) but not compressed files (such as PKLite and LZExe).

Scanning compressed and archived files will increase scanning time as files have to be decompressed first.

Scanning boot and partition sectors

By default, FindVirus scans boot and partition sectors on every disk. You can turn these checks off, but this is recommended only if an option is causing a problem; for example, if you are scanning a network drive which does not have a boot sector.

`/NOBOOT`	Stops FindVirus scanning the boot and partition sectors of the disk(s) specified.
`/NOPART`	Stops FindVirus scanning the partition sector of the disk(s) specified.

Producing reports

By default, FindVirus displays a report on the screen when it has finished its scan. A number of additional reporting options are available.

`/PRINTOUT`	Directs the report to the default system printer as well as to the screen.
`/REPORT=`*`file`*	Directs the report to the specified file as well as to the screen. The `/APPEND` switch appends the report to an existing file. If you only give a filename, the file is created in the default Toolkit directory.
`/LOUD`	Provides a more detailed report. As each file is scanned, the result is displayed on the screen

`/EVLOG` Report FindVirus activity to the NT event log. Scans create entries under the 'FindVirus' category, scans which find an infection also create an entry under the 'Infection' category.

`/BADLIST=`*`file`* Writes the names of suspect files, together with viruses, to the specified file. If you only give a filename, the file is created in the default Toolkit directory. To save it elsewhere, give a full pathname.

For example:

```
WFINDV32 C: /REPORT=VIRUS.REP /LOUD
```

scans the C: drive for viruses. As each file is scanned, its name is displayed on the screen. This detailed information is also written to a file called VIRUS.REP in the Toolkit directory.

Identifying viruses

`/MUTANT` Scans for slight variations of known viruses, known as mutants.

This option should be used with care as it can increase the possibility of false alarms. Most users do not need to use FindVirus with this option.

`/ANALYZE` Runs a heuristic scanner, looking for suspicious code that may be a warning of a new virus.

Use this option if you need extra security, for example if you use a large number of diskettes. It will increase scanning time.

Specifying actions

Switches can be set to request particular actions during or after a scan.

`/BEEP` Sounds a beep whenever a virus is encountered. By default, one beep is sounded at the end of the scan if any viruses have been detected.

`/ONVIRUS="`*`message`*`"` If this switch is set, FindVirus displays a message. The message must be in quotation marks and can contain any character except double quotation marks (") and forward slash (/), to a maximum of 40 characters.

For example:

```
WFINDV32 /LOCAL /ONVIRUS="Virus found.  Call PC
Support on 1234"
```

scans all local drives for viruses. If a virus is found, the warning message is output to the screen.

Network options

If you are using a PC on a network there are some additional options to allow a message to be sent to the administrator or member of support staff. The default is to send the following message to the network administrator:

```
<username> : Virus found on workstation!!!
```

where:

username is the name of the logged-on user.

The default message and the person to whom it is sent can be changed using the `/MSG` and `/TELL` switches.

`/MSG="`*`message`*`"`	Sends the specified message to the network administrator. The message must be in quotes and can contain any character except double quote (") and forward slash (/), to a maximum of 40 characters.
`/TELL=`*`name`*	Specifies the user to whom the message is sent. The name must be the network identifier of the recipient, such as a member of the support staff. The username can be in upper or lower case. You must use this switch in conjunction with `/MSG`.

For example:

```
WFINDV32 /ALLDRIVES /MSG="Urgent! A virus has
been found" /TELL=DSMITH
```

scans all hard drives, including network drives. If a virus is found, the specified message together with the username of the logged-on user is sent to DSMITH.

Users will only receive messages if they are logged in at the time.

Network messages can be prevented if required.

`/NOMSG`	Turns off all network messaging.

Defining drivers

When scanning, FindVirus uses a virus driver file called FINDVIRU.DRV which contains details of all current viruses. It also checks for an additional driver file called EXTRA.DRV which may contain details of more viruses. If additional drivers are provided by S&S, for example as an upgrade, you may need to use one of the following switches.

`/DRIVER=`*`file`* Instructs FindVirus to use the named virus driver file instead of FINDVIRU.DRV.

`/EXTRA=`*`file`* Instructs FindVirus to use the named additional driver file as well as of EXTRA.DRV.

Extra driver files are available from the S&S Bulletin Board.

Repairing files

To repair infected files, you can run FindVirus with the `/REPAIR` option.

Note: The Repair button on the user interface provides a straightforward way of repairing files, boot sectors and partition sectors. See Chapter 5, "Virus Repair and Removal".

`/REPAIR` Scan all files (as if the `/DOALLFILES` switch had been specified) and attempts to repair infected files. If a file cannot be repaired it is renamed and its file permissions set to prevent acccess by users without administrator privileges. Infected boot and partition sectors cannot be repaired.

/DELETE	The /DELETE switch causes FindVirus to delete any files that cannot be repaired, rather than renaming them. Before deleting the files, FindVirus overwrites them with zeroes to prevent anyone recovering them with an UNDELETE tool. You can only use the /DELETE switch in conjunction with the /REPAIR option.
/DELETE	The /DELETE switch causes FindVirus to delete any files that cannot be repaired, rather than renaming them. Before deleting the files, FindVirus overwrites them with zeroes to prevent anyone recovering them with an UNDELETE tool. You can only use the /DELETE switch in conjunction with the /REPAIR option.
/DISINFECT	Scan executable files and attempt to repair infected ones. If a file cannot be repaired it will be renamed and its file permissions set to prevent access by users without administrator privileges.
/DISINFECT /MOVE[=*path*]	Backs up files to the directory specified before a repair is attempted. If the infected file cannot be repaired the original is deleted. Backing up is highly recommended before an attempt is made to repair a file especially when checksum validation disinfection has failed. The backup can be deleted and purged once the repaired file had been confirmed as disinfected and intact.

For example:

```
WFINDV32 /LOCAL /REPAIR /DELETE
```

scans all local hard disks for viruses, and attempts to repair any infected files found. If any infected files cannot be recovered, they will be deleted. FindVirus will prompt for confirmation before deleting each file.

Note that NTFS does not allow files to be undeleted.

Requesting extended errorlevels

FindVirus returns an errorlevel after running. If you are writing batch files, you can request extended errorlevels, giving more information on errors.

`/EXTERROR`	Provides extended errorlevels, as explained in "Errorlevels" on page 90.

7.4 Hints and Tips

Errorlevels

FindVirus sets an errorlevel each time it runs. When writing batch files, you can use the ERRORLEVEL parameter on the IF command line to determine further actions.

The standard errorlevels are as follows:

Errorlevel	Meaning
255	Execution interrupted by user.
2	A virus was found.
1	A problem was encountered which was not a virus; for example, a file that could not be read.
0	No problems encountered.

You can request FindVirus to set extended errorlevels by using the `/EXTERROR` switch. These are as follows:

Errorlevel	Meaning
255	Execution interrupted by user.
48	File virus, virus dropper or virus test file found.
47	Partition sector virus found.
46	Boot sector virus found.
45	Virus found in memory.
44	Trojan found.
22	Driver file failed checksum.
21	Driver file not found.
20	Failed integrity check.

Errorlevel	Meaning
11	Joke program found.
10	Compressed files found.
1	A problem was encountered, which was not a virus. For example, a file which could not be read.
0	No problems encountered.

Hard disk device drivers

If your hard disk uses a utility such as Disk Manager, DoubleSpace, SpeedStor, Stacker, SuperStor or Vfeature to access it, you should boot from a diskette that loads the necessary software (usually a device driver) and run FindVirus to scan the C: drive first.

Scanning backup files

If you use FastBack or PCTools to make backups, FindVirus might report that the backup diskettes cannot be read. Because of the formatting, DOS cannot read the boot sector or any of the files on these diskettes.

If you have had a virus outbreak, you should assume that any unreadable diskettes are infected, and restore copies from a clean PC as soon as possible.

False alarms

Very occasionally, FindVirus may report a false alarm, that is, it may report a virus in a clean file. This occurs if the pattern of bytes found in a virus is also found in an uninfected file. The chances of a false alarm are increased slightly if you use the `/ANALYZE` option.

If you are in any doubt, contact your authorized distributor or S&S Technical Support.

7.5 Error messages

This section gives the most common error messages returned by FindVirus, with an explanation of why the error has occurred.

Cannot execute WFINDV32.EXE

There is insufficient memory for WFINDV32.EXE to load.

The program has been altered; please replace it with a good copy.

Changes have occurred to WFINDV32.EXE. Copy a clean version of the file from the Toolkit diskette.

Insufficient memory.

There is not enough memory for WFINDV32.EXE to execute.

Bad MESSAGES.DRV

The file MESSAGES.DRV is missing, or it has been altered. Check that the file is in the same directory as WFINDV32.EXE or replace it with a good copy from the original Toolkit diskette.

Bad driver FINDVIRU.DRV

The driver file FINDVIRU.DRV is missing, or it has been altered. Check that the file is in the same directory as WFINDV32.EXE or replace it with a good copy from the original Toolkit diskette.

This program is more than xx months old

FindVirus compares the system date with the date of FINDVIRU.DRV. If the difference is six months or more, FindVirus displays the "out-of-date" message. To insure you are fully protected from new viruses, you should subscribe to the regular upgrade service. See "Registration and upgrades" on page xi.

This page has been left blank

8. Advanced Virus Checking

This chapter provides detailed information on using ViVerify, including running the program from the command line or from within batch files.

8.1 How ViVerify works

ViVerify is a checksummer which is able to detect changes in executable files that may have been caused by a virus infection. ViVerify works by calculating a unique fingerprint for each file. This fingerprint is then recalculated when required, to check if there have been any changes.

Executable files

ViVerify only checks for changes in files most susceptible to virus infection. By default, it checks files with the following extensions:

APP	OV?
COM	SYS
DLL	XTP
EXE	386
FON	

Most executable files do not change, so any variation in the checksum may be an early warning of a virus infection. Occasionally, though, you may have an executable file that does change, or a data file that has one of the above file extensions. Specific individual files of this sort can be excluded from the checks. The following files are excluded by default:

CONFIG.SYS
WPQUE.SYS
WPSYSD.SYS
BOOTCONF.SYS
TELIX.FON

ViVerify also checks boot and partition sectors for changes.

Encryption algorithms

To create unique fingerprints (checksums) which cannot be detected by the virus, ViVerify uses an encryption algorithm.

The default algorithm used is the CCITT Cyclic Redundancy Check (CRC). This incorporates a user-specified keyword to increase security, and checks the files rapidly.

The Size algorithm calculates fingerprints based only on the size of the file. This is very quick, but can be fooled, or "spoofed", by some viruses.

The Checksum algorithm calculates fingerprints as a whole sum of the bytes checked in the files. It also incorporates the user-specified keyword.

The DES algorithm uses the standard Data Encryption Standard (DES) algorithm. This is the most secure option, but requires lengthy calculations, so it can slow down the checking.

Checking speed

By default, ViVerify speeds up the checking process by checking only the first and last 4 Kb of each file. This is known as turbo mode. If you need particularly high security, you can turn turbo mode off, allowing ViVerify to check the entire file.

However, it is very unlikely that a virus will infect a file without making changes to the beginning or end of the file.

To speed up checking further, ViVerify normally checks only every fifth byte in a file since it is difficult for a virus to infect a file without modifying at least one of the bytes checked by ViVerify. You can change this if you need greater security or faster checking on your system.

Running ViVerify

There are three stages to running ViVerify:

- Creating a list of the files to be checked for changes.
- Calculating fingerprints for these files.
- When required, recalculating the fingerprints to check for changes.

8.2 Running ViVerify from the user interface

You can run ViVerify from the Toolkit user interface in the following ways:

- By selecting the Check for Changes option on the main screen.
- By selecting Check for Changes from the Scan menu.

These options are explained in detail in Chapter 4. See "Checking for changes - ViVerify" on page 35.

8.3 Running ViVerify from the command line

You can run ViVerify directly from the command line by selecting Run from the File menu within Program Manager. You can also include the appropriate commands within a batch file.

Syntax

The standard command syntax is:

```
NTVIVERI function [switches]
```

where:

`function` is one of FILELIST, MAKEPRINT or CHECKPRINT.

FILELIST	Make a list of the files to check.
MAKEPRINT	Calculate the fingerprints for the listed files.
CHECKPRINT	Check the files in the list for changes.

The available switches are as follows:

Switch	Meaning
/BADLIST	Create a list of files that have changed.
/BEEP	Beep when a changed file is encountered.
/CRC	Use the CCITT Cyclic Redundancy Check algorithm (default).
/D=	Specify the drive(s) to be checked.
/DES	Use the DES algorithm.
/EXCLUDE=*file*	Exclude all files listed in specified file from fingerprinting or checking.
/EXTERROR	Provide extended error levels.
/FL=*file*	Create a file list (FILELIST function) or check files in list (MAKEPRINT or CHECKPRINT functions).
/FS=*file* /FPRINT=*file*	Define file holding the fingerprints.
/HOLDKEY	Wait for a keystroke before displaying the report.
/LOUD	Display status of each file checked.
/N=n	Check every nth byte of each file.
/NETVOL	Exclude unreadable network files from a file list.
/NT	Do not use turbo mode; check entire contents of file.

Switch	Meaning
/PRINTOUT	Output report to printer as well as to screen.
/REPORT=*file*	Output report to specified file as well as screen.
/SIZES	Use the file size algorithm.
/WHOLESUM	Use the whole sum algorithm.
/X=*keyword*	Specify the keyword to be used.
/YESBREAK	Enable interruption of ViVerify with Ctrl Break.

The available switches are explained in detail in the following sections. You cannot use any switch more than once on the command line. The switches must be separated by spaces, and they can be typed in upper or lower case.

Checking specific drives

When using any function, you should specify the drive(s) to be checked using the /D= switch.

/D=*drive* Indicates one or more drives to be checked.

Enter one or more of the identifying letters without spaces between them. Do not enter the colon. For example:

```
NTVIVERI /D=CD
```

will check the C: and D: drives.

You can also use a wildcard. For example:

```
NTVIVERI /D=*
```

will check all local drives.

Defining files to be checked

By default, ViVerify checks all executable files on the selected drive. When you use the FILELIST function, it will create a file containing a list of all the files to be checked. This file, normally called FILES.VVL, is subsequently used by the MAKEPRINT and CHECKPRINT functions.

If you want to check the contents of different drives separately, you can create separate file lists for each drive. In these circumstances, you should define particular file lists to be used, rather than using the default filename.

`/FL=`*`file`* With the `FILELIST` function, creates a file of the specified name to hold the list of files to be checked. With the MAKEPRINT and CHECKPRINT functions, checks all files listed in file.

For example:

```
NTVIVERI FILELIST /D=C /FL=C_FILES.VVL
```

creates a list of all the executable files on the C drive that are to be checked, and saves the list in a file called C_FILES.VVL in the default Toolkit directory.

Specifying a fingerprint file

When you use the MAKEPRINT function, the fingerprints created are stored in a file for future use by CHECKPRINT. By default, this file is called FINGERP.VVF. If you want to check the contents of different drives separately, you can create separate fingerprint files for each drive.

`/FS=`*`file`*
`/FPRINT=`*`file`* Specifies a particular file in which the fingerprints are saved.

You can use either the `/FS` switch or the `/FPRINT` switch; there is no difference.

For example:

```
NTVIVERI MAKEPRINT /FL=C_FILES.VVL
/FS=C_FPRINT.VVL
```

creates fingerprints for all files listed in the file C_FILES.VVL. (This assumes that the FILELIST function has already been run to create this list.) The fingerprints are saved in a file called C_FPRINT.VVL in the default Toolkit directory.

Remember that when you subsequently check the fingerprints using the CHECKPRINT function you must use the same file that you specified when you created the fingerprints.

Excluding files

ViVerify allows you to specify individual files which are not to be checked, for example executable files which you know are likely to change legitimately.

When it runs, ViVerify checks for a file called EXCLUDE.VVX in the Toolkit directory. If you have files that are likely to change legitimately, you can add them to EXCLUDE.VVX.

Alternatively, you can create a file containing the names of the files you want to exclude. This should be an ASCII file containing names of files that are not to be checked. File extensions should be included. If you do not provide a pathname, all occurrences of the file will be excluded.

If you use a file other than EXCLUDE.VVX, you must specify it using the `/EXCLUDE` option.

`/EXCLUDE=`*`file`*	Excludes from the checking process all files listed in the specified file.

Some network system files are inaccessible over a network. To insure that these are excluded from the file list, the `/NETVOL` switch should be used.

`/NETVOL`	Excludes all network system files inaccessible over a network.

Checking boot and partition sectors

By default, ViVerify checks the boot and partition sectors of every disk it examines. You can turn these checks off, but this is not recommended unless an option is causing a problem. For example, if you are checking a network drive which does not have a boot sector.

`/NOBOOT`	Stops ViVerify from checking the boot sectors.
`/NOPART`	Stops ViVerify from checking partition sectors.

Specifying a keyword

When you use the MAKEPRINT function, you must specify a keyword to be used in the fingerprinting algorithm (unless you are using the Size algorithm, which does not use a keyword.)

When you subsequently use the CHECKPRINT function on the same list of files, you must give the same keyword as a parameter.

`/X=`*`keyword`*	Specifies a keyword to be used when creating or checking fingerprints. The keyword must be at least eight alpha-numeric characters.

For example:

```
NTVIVERI AUTOMAKE /D=C /X=D5R2L0H7
```

will create a list of executable files on the C drive to be checked, and will create fingerprints for these listed files, incorporating the user-specified keyword.

Varying the checking speed and security

If you need a particularly high level of security, you can turn off turbo mode, forcing ViVerify to check the entire file instead of just the first and last 4 Kb.

`/NT`	Turns off turbo mode.

ViVerify normally checks every fifth byte in each file, which is sufficient for most users. You can set the program up to check more bytes, to provide greater security, or fewer bytes, for faster checking.

`/N=`*n*	Checks every nth byte in each file.

Specifying an algorithm

By default, ViVerify calculates fingerprints using the CCITT Cyclic Redundancy Check algorithm. This is suitable for most users, but you can specify a different algorithm if you specifically need greater security or increased checking speed.

`/SIZES`	Calculates fingerprints based on the file size.
`/CRC`	Uses the CCITT CRC algorithm (default).
`/WHOLESUM`	Calculates fingerprints as a whole sum of the bytes checked in the file.
`/DES`	Uses the Data Encryption Standard algorithm.

Defining actions

You can configure ViVerify to beep when it finds a changed file.

`/BEEP`	Beep when a changed file is found.
`/BIGBEEP`	Beep loudly when a changed file is found.

Producing reports

By default, ViVerify displays a report on the screen when you run the CHECKPRINT function. You can configure ViVerify to wait for a key to be pressed after the report is displayed.

`/HOLDKEY`	Wait for a keystroke after displaying the report.

You can also direct the report to a named file, to the default system printer or to both. You can specify whether the output appears in full or in a shortened form.

`/PRINTOUT`	Directs the report to the default system printer as well as to the screen.
`/REPORT=`*`file`*	Directs the report to the specified file as well as to the screen.
`/LOUD`	Provides a more detailed report. As each file is checked, its name is displayed on the screen.
`/QUIET`	Produces a report in a shortened form.

For example:

```
NTVIVERI CHECKPRINT /D=C /X=D5R2L0H7 /PRINTOUT
/LOUD
```

will recalculate fingerprints for executable files on the C drive, using the specified keyword in the encryption algorithm. As each file is checked for changes, its name is displayed on the screen, and the report is also sent to the default printer.

Extended errorlevels

ViVerify returns an errorlevel when it runs. You can request more detailed errorlevels for use in batch files if required. See "Errorlevels" on page 105.

`/EXTERROR`	Provide extended errorlevels.

Producing a list of suspect files

A list of changed files can be produced and written to a file. The contents of this file can then be checked by FindVirus, using the `/CHECKLIST` option. See "Scanning files and subdirectories" on page 81.

`/BADLIST=`*`file`* Writes a list of suspect files to the specified file. If you give just a filename, the file is created in the Toolkit directory. Alternatively, you can give a full path.

Errorlevels

ViVerify sets an errorlevel when the CHECKPRINT function is used. When writing batch files, you can use the ERRORLEVEL parameter on the IF command line to determine further actions.

The standard errorlevels are as follows:

Errorlevel	Meaning
255	Execution interrupted by user.
2	An executable file has been changed.
1	A problem was encountered which was not a virus; for example, a file that could not be read.
0	No problems encountered.

When the `/EXTERROR` switch is set, ViVerify sets the following extended errorlevels:

Errorlevel	Meaning
255	Execution interrupted by user.
4	Files have been deleted.
3	Invalid entry in fingerprint file.

Errorlevel	Meaning
2	An executable file has been changed.
1	File exists but could not be checked.
0	No problems encountered.

9. Toolkit Configuration

This chapter explains the configuration files which are used within the Toolkit.

9.1 The TOOLKIT.INI file

The TOOLKIT.INI file is used to hold a number of settings for the Toolkit programs. It is loaded automatically when you start the Toolkit. You can edit this file to customise it to your own installation, and you can create other files for different configurations, for example, for different users.

The file is divided into subsections, each of which starts with a heading in square brackets. Beneath each subsection is a list of options defining the current settings.

An example of the TOOLKIT.INI file is as follows:

```
[FindVirus]
Options=BEEP
Report=TOOLKIT.LST
List=FILES.VVL

[FileRepair]
Options=DELETE

[ViVerify]
Options=FILELIST SIZES
Report=VERIFY.REP
List=FILES.VVL
FPrint=FINGERP.VVF
Exclude=EXCLUDE.VVX
```

Note the following points about the format of the file:

- Do not include spaces.
- Where filenames are included, files are assumed to be in the standard Toolkit directory (default C:\WIN32APP\TOOLKIT) unless you give a full pathname.

The options that can be included are described below.

FindVirus

`Options=switches`	These can be any of the command line switches available for the WFINDV32 command. Do not include the slash character. Options containing an equals sign must be placed on separate lines.
`Report=`*`file`*	The output report file.
`List=`*`file`*	The file containing the list of files to be scanned.
`Driver=`*`file`*	The driver file to be used.

For more information on the available switches, see Chapter 7, "Advanced Virus Detection".

FileRepair

When FindVirus is run with the file repair option, it always tries to repair an infected file. If the file cannot be repaired, the file can either be renamed or deleted.

`Options=`	If you wish to rename files that cannot be repaired, specify RENAME. If you wish to delete files that cannot be repaired, specify DELETE.

ViVerify

`Options=switches`	Include any of the NTVIVERI command line switches. Do not include the slash character. Options containing an equals sign must be placed on separate lines.
`Report=`*`file`*	The output report file.
`List=`*`file`*	The file containing the list of files to be checked.
`Fprint=`*`file`*	The file containing the list of fingerprints.
`Exclude=`*`file`*	The file containing the list of files to be excluded from the check.

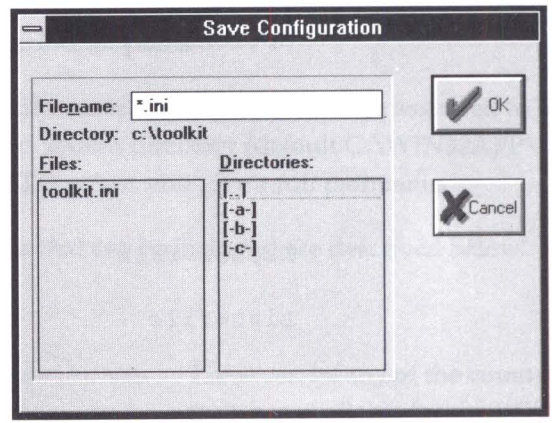
For more information on the available switches, see Chapter 8, "Advanced Virus Checking".

9.2 Configuration File Management

You can edit TOOLKIT.INI and FINDVIRU.INI using any text editor or word processor that can save the file as unformatted ASCII text.

Alternatively, you can load and save the configuration details held in TOOLKIT.INI from the user interface.

When you have set up a specific set of defaults for FindVirus and ViVerify you can save the settings in a configuration file. Select Save Configuration from the File menu. A file selector box of the following format is displayed:



Provide a name for the file to be saved, and select OK.

By default, the Toolkit loads TOOLKIT.INI when it starts up. To reload a different configuration file, containing previously saved settings, select Load Configuration from the File menu. Select or enter the name of the file to be saved and select OK. The file is loaded and the new settings are applied.

Glossary

alias	A different name by which a *virus* is known.
AUTOEXEC.NT	This file is run whenever a DOS box is launched from NT.
backup	A copy of your data held in another place in case your working copy is lost or damaged.
batch program	A file containing a set of commands that you can run by typing just one command. Batch files have the file extension BAT.
BBS	Bulletin Board System. An electronic mail system used to send messages and transfer files.
BIOS	Basic Input/Output System. Permanent programs that are used to load the operating system when the system is started up.
boot	Start the computer.
boot diskette	A diskette containing operating system files which can be used to start up your computer.
boot sector	The part of every hard disk and diskette that is read by the computer when it starts up.
boot sector virus	A virus transmitted in the *boot sector* of a diskette. Boot sector viruses infect the boot sectors of hard disks, and often the *partition sectors* as well.

bug	An unintentional fault in a program.
CARO	Computer Anti-Virus Researchers Organisation. Several S&S staff are members of CARO.
checksummer	A program that looks for viruses by checking for changes in *executable files*. ViVerify is an example of a checksummer.
clean	Free from viruses.
COM file	An *executable file* with a file extension of COM.
CONFIG.NT	This file is run whenever a DOS box is launched from NT.
defragmenters	A program which reorganises a hard disk so that different *clusters* of each file are stored contiguously if possible. This improves disk efficiency.
device driver	A program used to control the items of hardware connected to the PC such as disk drives and printers. .
directory	A logical subdivision of a disk which organises files into groups.
disk compressor	A program which stores files in a compressed form to maximise space on the hard disk.
dropper	A file which is not itself a virus, but infects the PC.
driver file	A file used by the Toolkit to enable the identification and reporting of viruses.

EICAR	European Institute for Computer Anti-Virus Research. S&S International is a member of EICAR.
EXE file	An *executable file* with the file extension EXE.
executable files	A program containing a program which can be run by typing its filename at the DOS command line or by double-clicking in Program Manager.
event log	A report file in Windows NT which can be used by applications to report on their status. This allows a users to find out what happened on a workstation at a particular time.
false alarm	A report of a virus where none exists.
fast infectors	A file virus that infects programs when they are opened or copied as well as when they are run.
file virus	A virus which infects *executable files*. When the program is run the virus copies itself. Most file viruses are *memory resident*.
fingerprint	A unique numeric identifier for a file; used by *checksummers* to check for changes in executable files. Also known as a checksum.
footbath PC	A PC used to check incoming files and diskettes for viruses. Also known as a *sheep-dip* PC.

format	The method of preparing a disk before files are written to it, using the FORMAT command.
GDE	Generic Decryption Engine. An element of FindVirus which enables it to identify even the most complex polymorphic encrypted viruses.
hexadecimal	Representation in base 16.
heuristic scanner	An element of FindVirus which checks files for suspicious code which may indicate a new virus.
infected file	A file containing a virus.
joke programs	Practical joke programs. These are not viruses, but sometimes a virus is contained in a joke program. The Toolkit detects joke programs.
logic bombs	A type of *trojan* that is triggered by a particular set of circumstances.
Master Boot Record	The partition sector of a hard disk.
memory resident	A program which remains in the PCs memory once it has run. Also known as *TSR*. NT does not allow memory-resident programs except device drivers and services.
multi-partite virus	A virus which uses a combination of techniques to spread, for example, infecting both files and *boot sectors*.
mutant	A slight variation of a known virus.
overwriting virus	A virus which overwrites each file it infects.

partition sector	The first part of a hard disk to be read. This contains the location of each partition, and the number of sectors in each one.
partition sector virus	A virus that replaces the normal *partition sector* of a hard disk.
polymorphic virus	A virus that tries to evade detection by scanners by ensuring that it does not have a fixed pattern of bytes. The Toolkit can detect polymorphic viruses using the Generic Decryption Engine.
public domain software	Software which you can copy and distribute legally.
root directory	The topmost directory on a disk, where all other directories and files are stored.
scanner	A virus detection program that searches for known viruses. FindVirus is an example of a scanner.
service	A small program which is loaded at the same time as the operating system and remains loaded until shutdown. Utilities such as the NT spooler and the NT computer browser are examples of a service.
shareware	Software which you can copy legally, but must pay for if you decide to use it.
sheep-dip PC	A PC used to check incoming files and diskettes for viruses. Sometimes called a footbath PC.

stealth	Characteristic of a virus which tries to avoid detection. Stealth viruses interfere with DOS and *BIOS interrupts* in order to conceal their presence.
SYS file	File, generally a *device driver*, with an extension of SYS.
time bombs	A type of *trojan* that is triggered by a particular date.
trojan	A program that has an unexpected action. Trojans are not viruses, as they do not replicate, but they are often damaging and are detected by the Toolkit.
TSR	Terminate and Stay Resident. A program that remains in memory after it has run. See *memory-resident*.
upgrade	A new version of the Toolkit which has been updated to detect newly-discovered viruses. Upgrades are available quarterly or monthly.
variant	A variation of a virus, usually caused by amending the code of an existing virus.
virus	A program that replicates itself.
write-protect	Ensuring that files cannot be written to a disk. A 5¼" diskette is write-protected by placing a label over the notch. A 3½" diskette is write-protected by sliding a plastic tab to uncover a hole.

Index

A
Advanced menu 25
algorithm 41, 103
aliases 6
anti-virus policy 10
archived files 32, 63, 74, 82
ARJ 32, 63, 82
autoloader 54

B
backup diskettes 91
backups 9, 10, 15
boot sector
    explanation 4
    FindVirus checks 83
    replacing 4, 47, 50, 51
    virus 3
    ViVerify checks 102
bugs 7
bulletin boards 7, 11

C
CARO 6
changed files 39
Check for Changes menu option 24
Checksum algorithm 42, 96
checksummers 12, 95
checksums 13, 35
clean-up operation 53
closing the Toolkit 23
CMOS 11
companion virus 4
compressed files 32, 63, 74, 82
Computer Anti-Virus Researchers Organisation 6
configuration file management 109
configuration files 31, 42, 107
conventions vii
CRC algorithm 41, 96, 103
Cyclic Redundancy Check. See CRC algorithm

D
Data Encryption Standard. See DES
data files 3
deleting files 49, 52
DES algorithm 42, 96, 103
disable event 59
disk space viii, 16
diskettes 6, 11, 50
DOS Toolkit viii, 46
downloading software 11
dropper 5

E
enable event 59
encrypted files 75
encryption algorithm 96
eradicating a virus 53
errorlevels
    FindVirus 89, 90
    ViVerify 105
event
    description 57
    disable 67
    editing 67
    enabling 67
    validating 67
event file 67
event log 68
executable files 74, 95
Exit menu option 24
EXTRA.DRV 87

F
false alarms 32, 91
File menu 24
file virus 2
Find Known Viruses menu option 24
FINDVIRU.INI
    editing 109
FindVirus
    advanced menu options 31
    command syntax 76
    configuration file 108
    driver file 87
    error messages 92
    errorlevels 90
    executable files 74
    hints and tips 90
    how it works 73
    network options 85

purpose 12, 27
repairing files 75
reporting 30, 83
running from the command line 76
running from the main screen 28
running from the user interface 30, 76
scanning specific drives 80
scanning specific files 81
Scheduler settings 63
switches 76
when to use 27
fingerprint 13, 35, 41, 95, 96

G
games 7, 12
Generic Decryption Engine 6

H
hardware requirements viii
help text 59
heuristic scanner 12, 64, 84
human error 9

I
installation
Scheduler 17
Toolkit 15
upgrades 19
installing the Toolkit 15

J
joke programs 9

K
keyboard 38
keyword 35, 102

L
Load Configuration menu option 24
loading configuration file 110
logic bomb 9
low-level programs 7
LZExe 32, 49, 64, 74, 82

M
main screen 23, 28
Master Boot Record 3
memory-resident 3
multipartite virus 5
mutants 32, 64, 84

N
network
virus infection 7
new virus 13, 47
Novell NetWare x
NTVIVERI command
functions 97
syntax 97

O
OS/2 x
overwriting virus 4

P
partition sector
explanation 3
FindVirus checks 83
ViVerify checks 102
partition sector viruses 3
pirated software 11
PKLite 32, 49, 64, 74, 82
PKZIP 32, 63, 74, 82
polymorphism 5

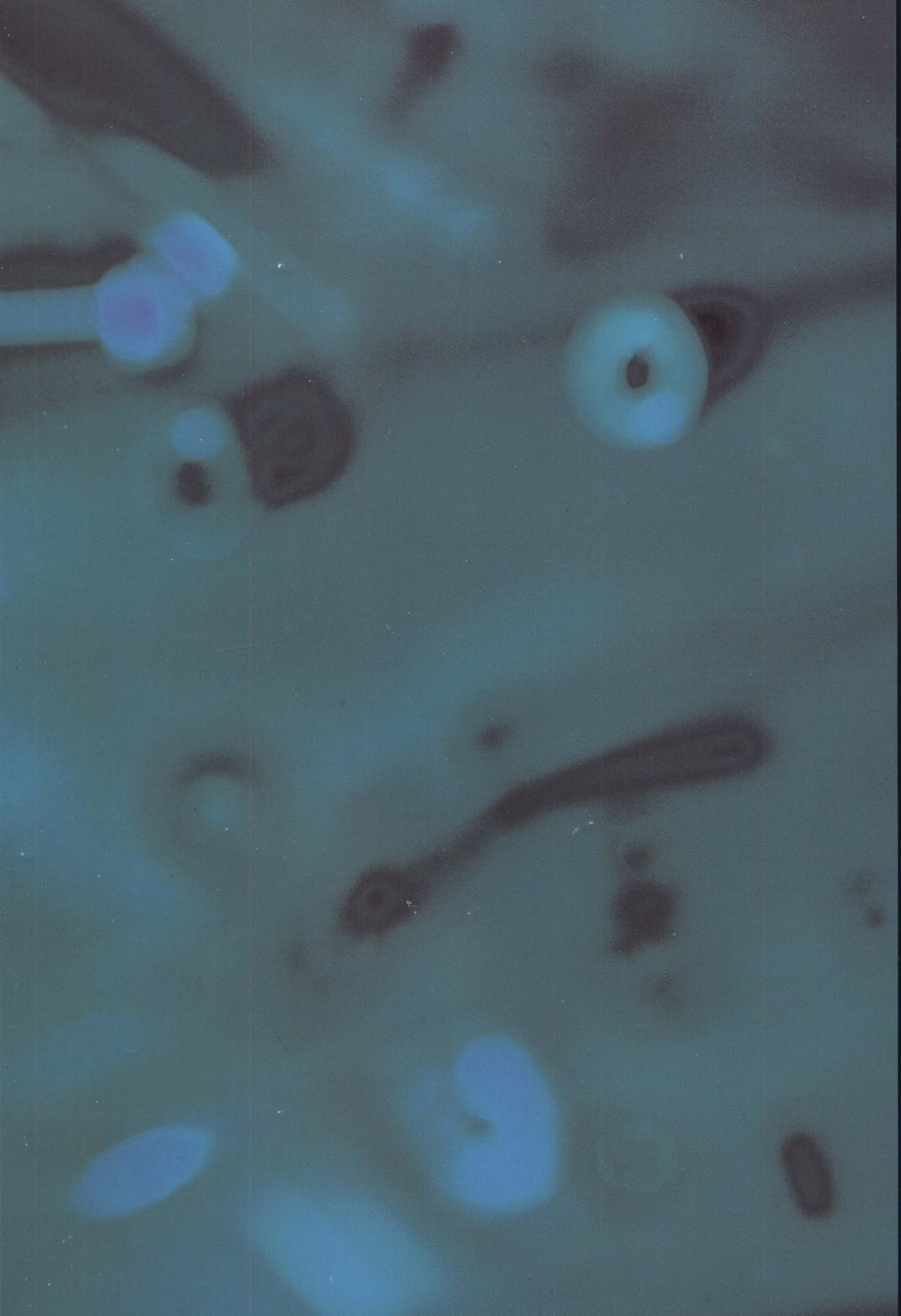
R
README files xiii, 8, 19
registration xii
renaming files 4, 46, 49
Repair File menu option 25
Repair menu 25, 48
repairing
files 48, 75, 87
from user interface 4, 46
single button 46
Replace Boot Sector menu option 25
replacing boot sectors 4, 47, 50
running an application 61

S
save configuration file 109
Save Configuration menu option 24
Scan menu 24
scanners 12
scanning specific files 81
Schedule Editor 58
Schedule menu option 25

Scheduler
adding an event 60
defaults 68
frequency settings 65
list boxes 71
scan settings 70
sending a message 62
shareware 7, 71
sheep-dip PC 13, 75
short-cut keys ix
Shred
menu option 24
running from the user interface 52
single-button repair 46, 50
Size algorithm 41, 96, 103
software requirements viii
software sources 11
spoofing 35, 96
status bar 68
stealth 5

T
technical support xiii, 19, 48, 91
time bomb 9
toolbar 21, 58
Toolkit
configuration 107
other versions x
program group 21
TOOLKIT.INI
editing 109
example 107
explanation 107
tooltips 68
trojans 8
turbo mode 42, 96, 103

U
unrepairable files 4, 46
upgrades xii, 19, 93
user interface 23

V
variants 6
virus
characteristics 5
definition 1
names 6
new 47
prevention 10
reporting 45
side effects 2
types 2
Virus Encyclopaedia x, 5, 13, 22, 43
Virus Encyclopaedia menu option 25
ViVerify
advanced menu options 40
algorithms 41, 96, 103
checking speed 96, 103
command line switches 99
computing fingerprints 37, 38
configuration file 109
creating file list 37
error levels 104
errorlevels 105
excluding files 41, 101
executable files 95
how it works 95
keyword 37, 102
purpose 13, 35
reporting 36, 104
running from the command line 97
running from the user interface 36, 97
suspect files 105
verifying fingerprints 37, 39
when to use 35
VIVERIFY command
switches 99

W
WFINDV32 command
switches 76
syntax 76
Windows icons 21